

# Online leeftijdsverificatie in Nederland

Marktverkenning



**ECP**

## Auteurs

Innopay

Nick Smaling & Jacob Boersma

## Uitgave

Versie 1.0

Februari 2013

Copyright © Innopay

Alle rechten voorbehouden

## Dankwoord

Graag willen wij iedereen bedanken die een bijdrage heeft geleverd aan de totstandkoming van deze marktverkenning. Allereerst alle personen die tijd beschikbaar hebben gemaakt voor interviews: deze verkenning was niet mogelijk geweest zonder jullie bijdragen. Verder willen wij Chiel Liezenberg, partner bij Innopay, bedanken voor zijn scherpe blik op de analyse. Tot slot bedanken wij Jaap Kuipers en het Platform Identity Management Nederland voor het beschikbaar stellen van relevante documentatie en de schat aan overige input voor deze studie.

## Inhoud

<b>Dankwoord</b> .....	<b>2</b>
<b>Inhoud</b> .....	<b>3</b>
<b>1 Managementsamenvatting</b> .....	<b>5</b>
<b>2 Inleiding</b> .....	<b>9</b>
2.1 Doel van het onderzoek .....	10
2.2 Leeswijzer .....	10
<b>3 Expertvisie op online leeftijdsverificatie</b> .....	<b>11</b>
3.1 Betrouwbaarheidsniveaus .....	11
3.2 Modellen in een tweezijdige markt .....	13
<b>4 Eisen en wensen van webwinkeliers</b> .....	<b>16</b>
4.1 Benodigde informatie .....	16
4.2 Wettelijk kader .....	16
4.3 Succesfactoren volgens webwinkelbranche .....	17
4.4 Randvoorwaarden en succesfactoren.....	18
<b>5 Het aanbod van leeftijdsverificatiediensten</b> .....	<b>20</b>
5.1 CDDN .....	20
5.2 DigiD .....	22
5.3 eHerkenning .....	23
5.4 eNIK/eRijbewijs .....	25
5.5 Experian.....	26
5.6 IDchecker.....	28
5.7 iDEAL .....	30
5.8 IRMA.....	31

5.9	Jumio .....	33
5.10	KPN .....	35
5.11	PostNL.....	35
5.12	Banken.....	37
<b>6</b>	<b>Analyse.....</b>	<b>38</b>
6.1	Betrouwbaarheid .....	38
6.2	Realisatietermijn .....	41
6.3	Huidige dekkingsgraad .....	41
6.4	Schaalbaarheid .....	42
6.5	Begrijpbaarheid / Gemak .....	42
6.6	Businessmodel.....	43
6.7	Privacy / Wetgeving .....	44
6.8	Veiligheid.....	44
6.9	Overzicht van de gehanteerde modellen.....	45
6.10	Samenvatting criteria en oplossingen.....	46
<b>7</b>	<b>Conclusie: vier ontwikkelrichtingen voor online leeftijdsverificatie .....</b>	<b>48</b>
7.1	Conclusie .....	48
7.2	Toekomstbeeld voor online identificatie .....	50
7.3	Aanbevelingen en vervolgstappen.....	52
	<b>Bijlage 1: Overzicht leeftijdsgebonden producten.....</b>	<b>53</b>

## 1 Managementsamenvatting

Welke oplossingen voor online leeftijdsverificatie zijn er op korte termijn in Nederland beschikbaar?

Dat is de vraag waar dit onderzoek een antwoord op geeft. Door een brede maatschappelijke en politieke discussie rondom het onderwerp zit het vraagstuk van leeftijdsverificatie in een stroomversnelling. Ook neemt de aandacht naar de online context toe. Wetgeving dwingt de verkoper van leeftijdsgebonden goederen en diensten om zekerheid te krijgen over de leeftijd van consumenten, ook in het online kanaal. In de praktijk blijkt dat dit niet of nauwelijks kan worden nageleefd door een gebrek aan een algemeen geaccepteerde systemen voor leeftijdsverificatie. Hierdoor ontstaat er een gedoogsituatie in afwachting van betere authenticatieoplossingen. De doelgroep waarnaar in dit onderzoek wordt gekeken zijn jongeren van 16-18 jaar, aangezien de meeste wettelijke leeftijdsgrenzen voor producten en diensten hierop van toepassing zijn (zie ook Bijlage 1).

Online leeftijdsverificatie is een specifieke vorm van elektronische identificatiediensten (e-ID) in het algemeen. In deze marktverkenning zijn twaalf verschillende potentiële e-ID oplossingen onderzocht die geschikt zijn voor online leeftijdsverificatie (*Experian, iDEAL, KPN, DigiD, CDDN, eHerkenning, PostNL, IRMA, Jumio, eNIK/eRijbewijs, IDchecker en Banken*). Deze oplossingen zijn vergeleken op acht verschillende randvoorwaarden en succesfactoren (*Begrijpbaarheid/Gemak, Betrouwbaarheid, Businessmodel/Betaalbaarheid van leeftijdsverificatie, Huidige dekkingsgraad, Privacy/Wetgeving, Realisatietermijn, Schaalbaarheid/Flexibiliteit en Veiligheid*).

Welke oplossingen kansrijk zijn wordt allereerst bepaald door het gewenste betrouwbaarheidsniveau. Het laagste niveau (Niveau 0) is zelfverklaring, dat wil zeggen dat consumenten claimen een bepaalde leeftijd te hebben zonder dat dit verder gecontroleerd kan worden. Eén niveau hoger (Niveau 1) bestaat uit vergelijken van persoonsgegevens met data die al elders bekend is, zogenaamde datavalidatie. Bij Niveau 2 is er sprake van authenticatie gebaseerd op een afgeleide identiteit, die ergens in het proces is gebaseerd op een wettelijk document. Het hoogste niveau tenslotte (Niveau 3) is een authenticatie direct gebaseerd op een wettelijk identiteitsdocument of -middel<sup>1</sup>.

Naast een keuze voor het vereiste betrouwbaarheidsniveau kan er een voor zijn voor de gewenste realisatietermijn. Direct beschikbare oplossingen bieden over het algemeen een

---

<sup>1</sup> De hier gehanteerde niveaus beslaan een breder spectrum van betrouwbaarheid dan STORK ([www.eid-stork.eu](http://www.eid-stork.eu)), een Europese standaard die een meer gedetailleerde onderverdeling maakt in niveaus van afgeleide identificatie (Niveau 2 in dit rapport).

lager betrouwbaarheidsniveau dan oplossingen die op dit moment nog in ontwikkeling zijn. Vervolgens is er nog gekeken naar de randvoorwaarden gesteld door de webwinkeliers. De branchevereniging voor webwinkels (Thuiswinkel.org) geeft aan dat een goede oplossing breed bereik binnen de doelgroep moet hebben en voldoende gebruiksvriendelijk moet zijn om conversie niet in de weg te staan.

Om succesvol te zijn moet een oplossing beschikbaar zijn tegen acceptabele kosten. Huidige dekkingsgraad, schaalbaarheid, begrijpbaarheid/gemak en betaalbaarheid zijn daarmee de belangrijkste criteria na betrouwbaarheid en realisatietermijn. Tenslotte dient een goede oplossing te voldoen aan wet en regelgeving voor privacy en aan minimale eisen voor informatiebeveiliging.

Bij het analyseren van de markt blijken er veel overeenkomsten te bestaan tussen online identiteitsoplossingen. Alle bekeken systemen zijn bijvoorbeeld geschikt voor een breder scala aan identiteitsdiensten dan alleen leeftijdsverificatie, bijvoorbeeld adresvalidatie. Een dergelijke brede propositie is een belangrijke succesfactor voor de langere termijn. Verder is het ook belangrijk dat er voldoende toegevoegde waarde wordt geleverd voor een acceptabele prijs. Ook dit business case-aspect wordt goed ingevuld door de meeste oplossingen: de (verwachte) vraagprijs staat in verhouding tot de aangeboden diensten. Daarnaast is het belangrijk dat de consument zijn eigen gegevens kan beheeren en dataminimalisatie de norm is. Deze vorm van privacy-by-design is belangrijk voor de privacy van de consument en de meeste oplossingen voldoen hier aan, of geven aan naar deze richting te bewegen. Datavalidatie diensten (niveau 1) zijn soms een uitzondering, maar deze diensten voldoen in ieder geval aan de eisen van de wet bescherming persoonsgegevens. Tot slot voldoen alle oplossingen aan de verwachte eisen voor informatiebeveiliging (al is dat bij de oplossingen die nog niet in de praktijk werken lastig na te gaan).

De keuze voor invoering van online leeftijdschecks in Nederland begint met een keuze voor het gewenste betrouwbaarheidsniveau. Hierbij zijn er verschillende scenario's:

- A. **Handhaven status quo.** De eerste mogelijkheid is om genoegen te nemen met de huidige zelfverklaringen (niveau 0). Dit betekent dat er niks verandert aan de huidige situatie en dat wordt doorgegaan met de manier waarop leeftijdsverificatie vandaag de dag gebeurt op het internet. Eventueel kan zelfverklaring worden aangevuld met controle bij levering in het geval van aankoop van fysieke goederen.
- B. **Quick win, best effort.** Indien er wordt gekozen voor datavalidatie als acceptabel betrouwbaarheidsniveau, kan op zeer korte termijn van start worden gegaan. Vooralnog dient dan genoegen genomen te worden met oplossingen die niet door de overheid zijn uitgegeven, maar wel met een korte realisatietermijn en potentieel groot bereik. Oplossingen die momenteel hiervoor geschikt zijn, zijn IDchecker, Experian, CDDN, en in de nabije toekomst KPN, PostNL en Jumio.

- C. Aanpassing van bestaande authenticatieproducten.** De derde optie is om alleen genoeg te nemen met oplossingen die gebaseerd zijn op een afgeleide authenticatie (waarbij ergens in het proces controle van een WID document heeft plaatsgevonden). Het meest kansrijk zijn dan de oplossingen die nu al bereik hebben, maar nog geschikt gemaakt moeten worden voor online leeftijdsverificatie zoals iDEAL en DigiD. Alternatieven kunnen zijn de hogere niveaus van eHerkenning, een netwerk dat al wel geschikt is voor allerhande vormen van online identificatie, maar op dit moment nog geen bereik heeft onder de doelgroep, of de IRMA kaart, die nog in ontwikkeling is. Het aanpassen van de systemen en/of registreren van voldoende gebruikers zal in alle gevallen zeker 1-2 jaar duren.
- D. Wettelijk verplicht middel op lange termijn.** Tot slot is de laatste mogelijkheid om alleen te kiezen voor het hoogste betrouwbaarheidsniveau en een wettelijk identificatiemiddel. Dit betekent wachten op de uitgifte van eNIK/eRijbewijs als middel voor leeftijdsverificatie. Op dit moment is nog niet te zeggen wanneer de eNIK geïntroduceerd wordt maar naar verwachting zal dit zeker nog 2-3 jaar duren en wellicht langer afhankelijk van het gekozen invoeringsscenario. Het is op dit moment ook nog in onderzoek of en hoe eNIK/eRijbewijs bruikbaar zullen zijn voor gebruik op mobiele apparaten.

Concluderend kan gesteld worden dat er bij de keuze van een oplossing een duidelijke keuze gemaakt moet worden voor een betrouwbaarheidsniveau enerzijds en een gewenste termijn voor realisatie anderzijds. Voor alle betrouwbaarheidsniveaus zijn één of meer systemen beschikbaar die voldoen aan minimale privacy- en beveiligingseisen en die een stap vooruit zijn ten opzichte van de huidige situatie (Scenario A). Het is dus zeker niet zo dat wachten op invoering van een overheidsmiddel de enige haalbare optie is voor online leeftijdsverificatie. Deze conclusie staat in scherp contrast met het recente antwoord op Kamervragen van het Ministerie van Justitie over dit onderwerp. Daarin werd aangegeven dat wachten op de eNIK de beste oplossing is, eventueel aangevuld met iDEAL. Deze marktverkenning toont aan dat er vele andere opties mogelijk zijn per direct of op korte termijn.

Oplossingen kunnen ook gemakkelijk naast elkaar bestaan of gecombineerd worden aangeboden door identity serviceproviders of in het samenwerkingsverband van een trust framework. Belangrijkste vervolgstappen voor verdere invoering van leeftijdsverificatie zijn:

1. Duidelijkheid vanuit de wetgever over de eisen aan webwinkeliers. Wordt de huidige gedoogconstructie wel of niet gehandhaafd?
2. Gebruiksgemak en bereik zijn cruciaal voor succesvolle oplossingen.
3. Goede businesscase. De kosten van een verificatie moeten per transactie laag blijven ten opzichte van het transactiebedrag.

4. Uitbreidbaarheid naar andere identificatiediensten. De onderzochte oplossingen bieden deze mogelijkheid, maar deze diensten moeten nog wel verder uitgewerkt worden.

Uit het onderzoek volgen een viertal aanbevelingen:

1. Een eerste aanbeveling is om verschillende opties verder uit te werken waarlangs leeftijdsverificatie zich kan ontwikkelen. Na deze eerste marktverkenning van de aanbodkant van e-identity is het nuttig om dieper in te gaan op de vraagkant: welke van de bekeken factoren zijn echt kritieke succesfactoren voor consumenten en webwinkels? Welke combinaties van oplossingen zijn mogelijk?
2. Een tweede aanbeveling is om de marktverkenning uit te breiden naar overige oplossingen. Hoewel dit rapport een representatief beeld geeft, verdient het aanbeveling om ook andere Nederlandse oplossingen nader te bekijken zoals van Qiy ([www.qiy.nl](http://www.qiy.nl)) en Prooflink ([www.prooflink.com](http://www.prooflink.com)). Daarnaast moeten oplossingen die in het ons omringende buitenland gebruikt worden ook niet vergeten worden.
3. De derde aanbeveling richt zich op de overheid. De overheid moet duidelijke eisen formuleren aan private initiatieven op gebied van leeftijdsverificatie en e-identity en duidelijkheid scheppen over beoogde handhaving van (web)winkels en online dienstverleners.
4. Tot slot is het belangrijk om de maatschappelijke discussie te voeren over leeftijdsverificatie op internet. Tot nu toe wordt die geblokkeerd doordat partijen wachten op overheidsoplossingen (eNIK/eRijbewijs) en in de tussentijd genoeg nemen met zelfverklaringen of andere beperkte toepasbare maatregelen. Pilots/Proof of Concept projecten kunnen hiervoor input leveren. Als platform voor bedrijfsleven, overheid en internetsamenleving kan ECP een belangrijke aanjagende rol vervullen in de discussie.



## 2 Inleiding

Het vraagstuk van leeftijdsverificatie op internet zit in een stroomversnelling: de Tweede Kamer heeft zich uitgesproken voor verhoging van de leeftijd van alcoholverkoop en aanscherping van controles<sup>2</sup> en websites als Uitzending Gemist worden gedwongen tot het beperken van kijkmogelijkheden voor leeftijdsgebonden materiaal<sup>3</sup>.

Webwinkeliers en andere online dienstverleners lijken op dit moment geen mogelijkheden te hebben om op een betrouwbare en betaalbare manier aan de wettelijke verplichtingen en wensen voor leeftijdscontrole te voldoen. Daarmee zijn de webwinkeliers de probleemeigenaar. Wetgeving dwingt hen ertoe om leeftijdsverificatie uit te voeren voor leeftijdsgebonden goederen en diensten. Het vragen van een kopie WID-document is onwenselijk vanuit privacy-oogpunt, technische oplossingen vanuit de overheid laten nog op zich wachten. Het huidige beleid is om de dienstverlening dan maar te gedogen zonder dat gedegen leeftijdschecks plaatsvinden. Dit is evengoed onwenselijk vanuit maatschappelijk oogpunt en creëert rechtsongelijkheid tussen online en fysieke winkels.

In een reactie op Kamervragen meldde het Ministerie van Veiligheid en Justitie op 22 augustus 2012 het volgende over online leeftijdsverificatie in Nederland:

*‘Een bijzonder aspect bij de bescherming van jongeren tegen mogelijk schadelijk beeldmateriaal vormt de verstrekking daarvan via het internet. Naleving van de leeftijdsgrenzen is daarbij problematisch vanwege het ontbreken van direct fysiek contact tussen de verstrekker en de klant. Deze problematiek speelt niet alleen bij de verkoop van films en games, maar ook bij andere leeftijdsgebonden producten waaronder alcohol en tabak. Daarom zijn de ministeries van VWS en Veiligheid en Justitie in 2010 samen gestart met het inventariseren van de criteria en mogelijkheden voor een betere controle op de leeftijd bij verkoop van deze producten en diensten via internet. Uit deze inventarisatie, waarvan in de bijlage bij deze brief uitgebreid verslag wordt gedaan, blijkt dat de meest kansrijke optie thans de controle biedt via de introductie van de elektronische Nederlandse Identiteitskaart (eNIK). Een werkbaar alternatief biedt de leeftijdscontrole via iDEAL, zij het dat deze optie niet honderd procent dekkend is.*

<sup>2</sup> 09-07-2012 <http://www.nu.nl/politiek/2853931/kamer-wil-alcoholleeftijd-18-jaar.html>

<sup>3</sup> 26-04-2012 <http://www.publiekeomroep.nl/organisatie/pers/artikelen/16-programma%E2%80%99s-uitzending-gemist-alleen-na-22-uur?page=10>

De inzet van het ministerie op eNIK en eventueel iDEAL betekent dat er op korte termijn nog geen oplossing beschikbaar zal zijn voor webwinkeliers. Dit onderzoek wil breder kijken naar andere mogelijke oplossingen naast de genoemde twee en aantonen dat er veel meer mogelijkheden zijn waar gebruik van gemaakt kan worden. De bekeken oplossingen worden vergeleken met elkaar en met de eNIK en iDEAL op een aantal criteria.

## **2.1 Doel van het onderzoek**

Deze marketverkenning is uitgevoerd door Innopay in opdracht van ECP, het Platform voor de Informatiesamenleving, om verschillende beschikbare oplossingen voor online leeftijdsverificatie in Nederland in kaart te brengen. Het doel van het project is dan ook om antwoord te kunnen geven op de vraag:

*Welke oplossingen voor online leeftijdsverificatie zijn op korte termijn in Nederland beschikbaar?*

## **2.2 Leeswijzer**

Het rapport begint met onze expertvisie op het vraagstuk van leeftijdsverificatie. Dit hoofdstuk definieert ook de begrippen die in het rapport en in het bredere vakgebied van online identiteit gebruikt worden. Vervolgens wordt de vraagkant van de markt beschreven.

Hoofdstuk 3 richt zich op de vertrouwende partijen, de webwinkeliers en online dienstverleners, en analyseert welke wensen en eisen zij stellen aan een goede en betrouwbare oplossing. Hier is Thuiswinkel.org, de branchevereniging voor webwinkeliers, geraadpleegd. De verschillende criteria worden bekeken en het kader wordt geschetst waarop oplossingen zijn getoetst.

Vervolgens worden in hoofdstuk 4 alle individuele oplossingen die onderzocht zijn beschreven. Dit is een doorsnede van de aanbodkant van de markt die reeds actief is, of potentieel actief gaat worden, in diensten voor online leeftijdsverificatie in Nederland.

Hoofdstuk 5 gebruikt het conceptueel kader uit hoofdstuk 3 om de oplossingen met elkaar te vergelijken.

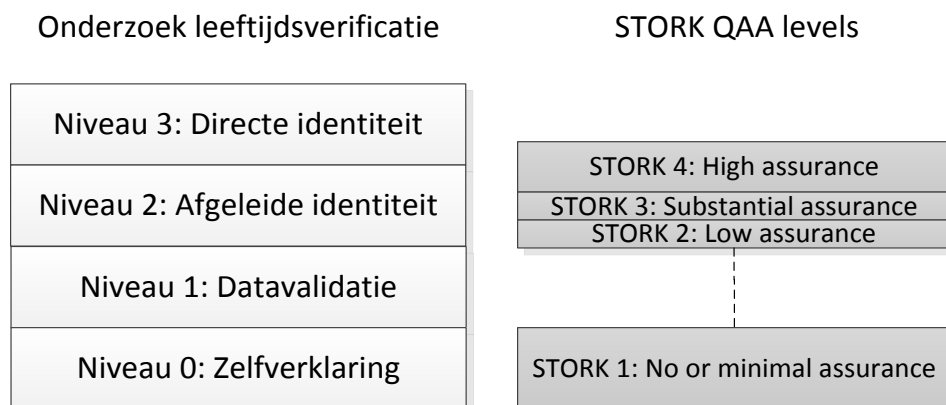
Tot slot bevat hoofdstuk 6 de conclusie van het onderzoek, waarin de oplossingen worden toegelicht. Ook worden aanbevelingen gedaan voor het vervolg.

### 3 Expertisie op online leeftijdsverificatie

Online leeftijdsverificatie gaat over het op afstand vast kunnen stellen van identiteit, ook al zijn we maar geïnteresseerd in een klein onderdeel daarvan ('is deze consument wel of niet ouder dan 16/18 jaar?<sup>4</sup>'). Dit hoofdstuk gaat in op hoe Innopay tegen het probleem van online leeftijdsverificatie aankijkt. Een belangrijke kanttekening is dat leeftijd weliswaar een attribuut is van een identiteit, en online leeftijdsverificatie slechts één context, maar dat de visie ook van toepassing is op andere attributen van de identiteit van een persoon.

#### 3.1 Betrouwbaarheidsniveaus

Er zijn vier verschillende niveaus van betrouwbaarheid te definiëren voor het online vaststellen van een identiteit. Deze niveaus geven de kans aan dat de persoon die zich identificeert ook daadwerkelijke de consument is of daadwerkelijk aan het leeftijdscriterium voldoet. Dit is een belangrijk onderwerp, omdat er een keuze zal moeten worden gemaakt welk niveau goed genoeg wordt bevonden voor online leeftijdsverificatie in Nederland. De door ons gedefinieerde betrouwbaarheidsniveaus hebben een samenhang met de internationale STORK QAA levels, maar voegen een datavalidatieniveau toe tussen 'no assurance' en het laagste niveau van afgeleide identiteitscontrole. Verder wordt er een hoogste niveau toegevoegd specifiek voor door de overheid uitgegeven identiteitsbewijzen (in STORK bestaat niveau 4 uit zowel overheidsmiddelen als privaat uitgegeven middelen).



Figuur 1: Betrouwbaarheidsniveaus marktverkenning leeftijdsverificatie in vergelijking met STORK ([www.eid-stork.eu](http://www.eid-stork.eu))

<sup>4</sup> Hoewel er diensten te bedenken zijn voor andere leeftijdsgrenzen (wel/geen 65+, onder de 14 voor toegang tot een jeugdforum, etc.) richt dit onderzoek zich specifiek op leeftijdsverificatie voor de grens van 16 of 18 jaar omdat die voor veel goederen en diensten is vastgelegd in wet- en regelgeving bedoeld voor de bescherming van jongeren.

### **3.1.1 Niveau 0: Zelfverklaring**

Het laagst mogelijke niveau (Niveau 0) is het niveau van zelfverklaring. Hierbij geeft de consument een eigenverklaring over een aspect van zijn identiteit. In het specifieke geval van leeftijdsverificatie beweert de consument zelf dat hij de leeftijd van 16 of 18 al heeft bereikt, zonder controle door een derde partij. Het risico ligt hierbij volledig bij de webwinkelier, aangezien die verantwoording af moet leggen mocht de consument niet de juiste leeftijd hebben ingevuld. Toch is dit in veel gevallen de enige manier van verificatie die wordt gebruikt. Dit niveau komt overeen met STORK 0, waarbij er geen of minimale assurance is.

### **3.1.2 Niveau 1: Datavalidatie**

Niveau 1 is datavalidatie van bekende gegevens van de consument. De consument voert zijn gegevens in op de website van webwinkelier en deze worden gecontroleerd door deze gegevens te valideren tegen gegevens in een (externe) database. Als de naam en adres en geboortedatum bijvoorbeeld overeenkomen met gegevens die bekend zijn bij een telefoonmaatschappij of energieleverancier dan mag er met een hogere mate van zekerheid van uit worden gegaan dat deze gegevens juist zijn.

Op zijn minst is deze methode een check op de consistentie van eerder afgegeven zelfverklaringen bij andere leveranciers, maar indien de gecontroleerde bron eerder een check heeft gedaan op een wettelijk identificatiemiddel dan benadert deze methode het betrouwbaarheidsniveau van Niveau 2.

Het is hierbij wel mogelijk om gegevens van een ander in te vullen, als de persoonsgegevens van die persoon bekend zijn, en zo identiteitsfraude te plegen. De controle op de data lijkt dan te kloppen terwijl er een ander persoon de bestelling heeft gedaan. De zekerheid kan verhoogd worden door ook rekening te houden met bijvoorbeeld een afleveradres.

### **3.1.3 Niveau 2: Afgeleide identiteit**

Niveau 2 omvat methodes die gebruik maken van een afgeleide identiteit van een persoon, dat wil zeggen dat de persoon zich identificeert met behulp van een middel dat aan hem is uitgereikt op basis van controle van een wettelijk identificatiemiddel. Het grote verschil met datavalidatie is dat voor een identificatie op dit niveau vereist is dat de consument een handeling verricht die alleen hij kan doen, bijvoorbeeld het invoeren van een geheime pincode of wachtwoord, of het aanbieden van een smartcard die alleen hij bezit. De webwinkelier kan er dus van uit gaan dat de consument zich identificeert met een middel welke ook daadwerkelijk hoort bij deze persoon en onder diens uitsluitende controle is.

Een voorbeeld hiervan is een bankpas, welke een persoonsgebonden middel is, uitgereikt tijdens een fysiek uitgifteproces. Het is nog steeds mogelijk om identiteitsfraude te plegen

door de middelen en gegevens van een andere persoon te gebruiken, maar dit is al een stuk moeilijker omdat ook wachtwoorden, pincodes of persoonlijke passen moeten worden gestolen of onderschept.

Binnen de STORK standaard wordt dit niveau verder opgedeeld in STORK 2, 3 en 4 afhankelijk van de niveaus van identiteitscontrole en veiligheid van het middel.

### **3.1.4 Niveau 3: Directe identiteit**

Het hoogste niveau (Niveau 3) is een vorm van directe identiteitscontrole met behulp van een wettelijk identificatiemiddel. Dit is een middel dat voldoet aan de wettelijke eisen aan identificatiedocumenten (WID-document). Een voorbeeld hiervan is een paspoort of een rijbewijs dat door de overheid is versterkt op basis van gegevens uit de GBA. Wanneer een consument zich identificeert met zijn fysiek, door de overheid uitgegeven middel, kan de (web)winkelier met grote mate van zekerheid aannemen dat dit ook de persoon is die de consument zegt te zijn. Zelfs hier is de zekerheid niet absoluut omdat identiteitsbewijzen vervalst of gestolen kunnen zijn. Aanvullende maatregelen zijn de controle van (digitale) echtheidskenmerken en/of checks in databases van gestolen WID-documenten.

Gedeeltelijk komt dit overeen met level 4 in de STORK standaard, maar STORK 4 omvat ook privaat uitgegeven middelen die gebaseerd zijn op controle van een WID-document.

## **3.2 Modellen in een tweezijdige markt**

Naast de indeling in betrouwbaarheidsniveaus kunnen oplossingen ingedeeld worden in verschillende organisatievormen.

Online leeftijdsverificatie heeft alle karakteristieken van een tweezijdige markt. Hiermee bedoelen we dat de twee betrokken actoren, de consumenten en de webwinkeliers, voor het uitvoeren van de leeftijdsverificatie duidelijk verschillende behoeften hebben, die op hun beurt weer met verschillende diensten worden ingevuld. In dergelijke markten bestaan netwerkeffecten: hoe meer consumenten een oplossing gebruiken, hoe interessanter het voor een webwinkelier is om erop aan te sluiten. Andersom is het voor consumenten interessanter om mee te doen naarmate er meer webwinkels van een oplossing gebruik maken.

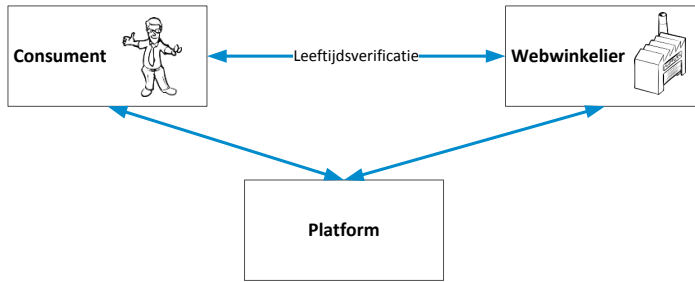
Er zijn in principe drie modellen om een tweezijdige markt mee te faciliteren: direct, platform en Trust Framework. De verschillende vormen van leeftijdsverificatieoplossingen die vallen binnen de betrouwbaarheidsniveaus 1, 2 en 3, zoals beschreven in 3.1, kunnen worden ingedeeld langs deze drie modellen. Het niveau van zelfverklaring volgt vanzelfsprekend altijd het directe model, omdat de consument zelf aangeeft dat hij de leeftijd al heeft bereikt zonder controle door een derde partij.

- **Direct.** Een direct model is een model waar er een-op-een koppeling is tussen de webwinkelier en de consument zonder dat daar een derde partij bijkomt. In het specifieke geval van online leeftijdsverificatie betekent dat, dat de consument zonder tussenpersoon direct in verbinding staat met de webwinkelier om zijn leeftijd te laten verifiëren met een middel of methode die door de webwinkelier is uitgegeven. Niveau 3 van betrouwbaarheid kan hier niet mee worden ondersteund omdat dit altijd afhankelijk is van een derde partij (namelijk de overheid) als uitgever van het wettelijk middel. Voordeel van de directe identificatiemethode is dat de winkelier zich niet hoeft aan te sluiten bij andere systemen en zo zeer flexibel is. Nadeel voor de consument is dat hij mogelijk voor iedere winkelier opnieuw een middel moet aanschaffen of zich moet registreren. Nadeel voor de winkelier is dat hij zelf het wiel moet uitvinden.



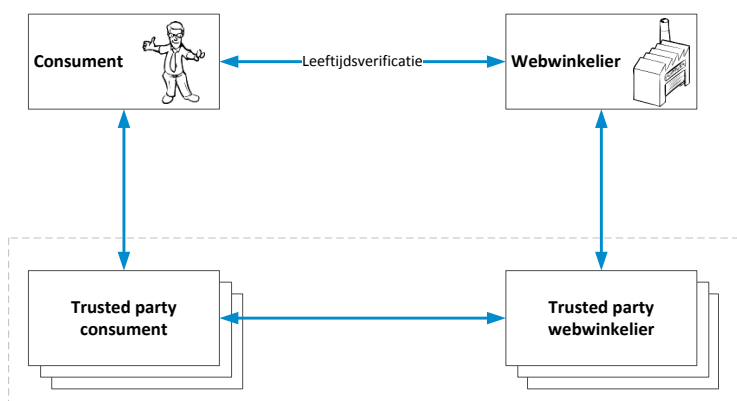
**Figuur 2: Direct model voor leeftijdsverificatie**

- **Platform.** Het platform is een vorm waarbij consument en winkelier gebruik maken van een identificatieplatform waar ze beide bij aangesloten zijn. Het platform doet richting de webwinkelier een uitspraak over de identiteit van de consument en treedt zo op als ‘trusted third party’. De betrouwbaarheid van de uitspraak van het platform is afhankelijk van de betrouwbaarheid waarmee het platform zelf de identiteit van de consument heeft vastgesteld bij registratie. Een bekend voorbeeld van een online platform met een hoog bereik maar twijfelachtig niveau van betrouwbaarheid is Facebook. Het voordeel van een platform voor winkeliers is dat er veel identificatiewerk uit handen wordt genomen en dat er gebruik gemaakt kan worden van de expertise van het platform. Een voordeel voor de consument is dat hij nu terecht kan bij alle webwinkeliers die op dit platform zijn aangesloten. Nadeel voor winkeliers is dat ze de (technische) aansluiting op het platform moeten realiseren, en indien niet alle consumenten bij hetzelfde platform zitten potentieel meerdere platforms zullen moeten ondersteunen. Het is een nadeel voor de consument als niet alle webwinkeliers bij één platform zijn aangesloten, daarnaast kan het een bedreiging voor de privacy zijn als één groot platform het monopolie krijgt op een groot deel van de identiteitstransacties.



**Figuur 3: Platform model voor leeftijdsverificatie**

- **Trust Framework.** De laatste variant van modellen voor identiteitsverificatie is een Trust Framework. Dit is een vierpartijenmodel, zoals dat bijvoorbeeld ook in de creditcardwereld gehanteerd wordt. Er is in dit geval dus geen centraal platform meer, maar de consument en de webwinkelier hebben beide een eigen trusted party en al deze bedrijven werken met elkaar samen in een afsprakenstelsel, het Trust Framework. Een Trust Framework bestaat uit gemeenschappelijk afspraken welke tussen partijen worden gemaakt over de onderlinge connecties, om vertrouwen te genereren en bereik te maximaliseren. Het bereik van het afsprakenstelsel is in onderstaande figuur aangegeven met stippelijntjes. Voordeel voor consumenten en webwinkeliers is dat de identificatie plaats kan vinden ongeacht de partij waar zij bij zijn aangesloten voor hun middel of dienst, mits deze participeren in het Trust Framework. Nadeel is dat het organiseren van een vierpartijenmodel veel inspanning kost en beheer vereist van het onderlinge afsprakenstelsel. Ook moeten er afspraken worden gemaakt over het verrekenen van kosten (businessmodel) tussen de verschillende partijen in het model. Zolang de markt voor online leeftijdsverificatie klein is zal het dus moeite kosten om hiervoor een afsprakenstelsel op te zetten, tenzij wordt meegelift op een bestaand afsprakenstelsel/Trust Framework zoals eHerkenning<sup>5</sup>.



**Figuur 4: Trust Framework voor leeftijdsverificatie**

<sup>5</sup> Zie [www.eherkenning.nl](http://www.eherkenning.nl)

## 4 Eisen en wensen van webwinkeliers

Naast de theoretische mogelijkheden voor betrouwbaarheidsniveaus en organisatievormen moet er ook rekening worden gehouden met de praktische overwegingen van gebruikers van online identificatiediensten: de webwinkeliers.

Winkeliers en dienstverleners zijn wettelijk verplicht tot het uitvoeren van leeftijdscontroles bij het leveren van leeftijdsgebonden producten en diensten. Op 10 februari 2009 is er door de overheid met de audiovisuele branche een convenant gesloten waarin afgesproken is om de handhaving op leeftijdsgebonden producten te verbeteren. Op 28 oktober 2009 is een zelfde convenant ondertekend met de (winkel)ketens die marktleider zijn in hun sector. Voor webwinkeliers bestaat een dergelijk convenant nog niet. In dit hoofdstuk wordt uitgediept wat webwinkeliers en online dienstverleners verwachten van een oplossing op het gebied van online leeftijdsverificatie.

### 4.1 Benodigde informatie

Een eerste inventarisatiestap is het in kaart brengen van leeftijdsgebonden producten en diensten in Nederland. In Bijlage I is een overzicht te vinden van soorten producten/diensten en de minimaal benodigde informatie, die nodig is voor een rechtmatige of wenselijke verkoop van het product of de dienst. Hiermee wordt bedoeld: welke informatie heeft een bedrijf ten minste nodig van de klant om het product te mogen verkopen. Behoort de winkelier alleen te weten of zijn of haar klant boven de achttien jaar is, of is er ook andere informatie noodzakelijk? Hierbij kan gedacht worden aan de exacte leeftijd, de woonplaats, een BKR goedkeuring of een burger service nummer (BSN).

### 4.2 Wettelijk kader

De huidige stand van zaken op het gebied van leeftijdsverificatie is dat bedrijven wettelijk verplicht zijn tot het controleren van de leeftijd van hun afnemers indien voor hun producten of diensten een leeftijdsgrens geldt. Er wordt in de wet niet gedifferentieerd tussen de offline en de online wereld. Dit betekent dat er een identificatieplicht ligt bij de webwinkelier. Webwinkeliers vullen deze plicht nu in op verschillende manieren maar deze zijn verre van ideaal. Enkele voorbeelden zijn:

- *Controleren van de leeftijd door de bezorger op het moment dat de goederen worden afgeleverd.* Dit kan ertoe leiden dat een transactie alsnog niet wordt voltooid ook al zijn de kosten voor bezorging al gemaakt. Ook is deze controle alleen uit te voeren bij fysieke levering.



- Registratie van de onderneming in het buitenland waar minder strenge regels gelden (specifiek voor online diensten, niet voor fysieke goederen).
- Vragen aan de gebruiker om een zelfverklaring. Bijvoorbeeld met een vinkje aangeven dat hij/zij ouder is dan 16/18 jaar of door invullen van de geboortedatum.
- Vragen om kopie van paspoort of rijbewijs op te sturen naar het bedrijf. Dit is onwenselijk omdat een dergelijke kopie veel meer informatie bevat dan nodig voor voltooiing van de transactie. Bovendien vertraagt het de transactie aanzienlijk vanwege de vereiste handmatige handelingen.
- Alleen toestaan van betaling met creditcard (omdat creditcards niet beneden de 18 jaar worden uitgegeven). Dit beperkt echter wel sterk de potentiële klantenkring, aangezien niet iedereen boven de 18 zal beschikken over een creditcard.
- Geheel niet vragen naar de geboortedatum/leeftijd.

### 4.3 Succesfactoren volgens webwinkelbranche

In de onderstaande tabel 1 staan randvoorwaarden en succesfactoren voor online leeftijdsverificatiediensten. Aan Thuiswinkel.org<sup>6</sup>, de branchevereniging voor webwinkeliers, is gevraagd aan te geven wat zij belangrijk vinden aan een eventuele oplossing. Het antwoord luidt als volgt:

*‘Voor producten als alcohol en games geldt in winkels een identificatieplicht. Webwinkels willen hier ook graag aan voldoen. Er zijn allerlei diensten op de markt voor online identiteit, maar geen enkele levert een wettelijk geldige leeftijdscheck op. Webwinkels zijn al een tijd op zoek naar een manier om zekerheid te verkrijgen over bepaalde eigenschappen van klanten. Het gaat dan bijvoorbeeld om de naam of het adres, maar ook om de leeftijd. Wanneer het gaat om het voldoen aan wettelijke eisen, kijken webwinkels in eerste instantie uit naar een situatie die vergelijkbaar is in de wereld van traditionele retail, waar klanten zich identificeren met een door de overheid uitgegeven middel.’*

Wanneer gevraagd wordt naar de specifieke eisen aan een identiteitsdienst gelden voor webwinkels in grote lijnen dezelfde eisen als bij betaalmiddelen: ‘oplossingen moeten **bereik** en **conversie** bieden tegen **acceptabele kosten**.’

---

<sup>6</sup> Zie [www.thuiswinkel.org](http://www.thuiswinkel.org)

#### 4.4 Randvoorwaarden en succesfactoren

Er zijn acht belangrijke factoren die kunnen worden bekeken bij potentiële oplossingen voor leeftijdsverificatie, te weten: Betrouwbaarheid, Realisatietermijn, Huidige dekkingsgraad, Schaalbaarheid/Flexibiliteit, Begrijpbaarheid/Gemak, Businessmodel/Betaalbaarheid van leeftijdsverificatie, Privacy/Wetgeving en Veiligheid. Deze zijn gebaseerd op de criteria geformuleerd in de werkgroep Internetverkopen<sup>7</sup> aangevuld met belangrijke criteria om de inzetbaarheid op korte termijn van een oplossing te kunnen bepalen.

Alle oplossingen moeten minimaal voldoen aan geldende wet- en regelgeving en een acceptabele Veiligheid, daarom zijn deze aspecten als minst onderscheidend onderaan de criterialijst gezet. Het te kiezen betrouwbaarheidsniveau zoals beschreven in het vorige hoofdstuk is de basis van een te kiezen oplossing en is daarom bovenaan gezet. Over het te hanteren betrouwbaarheidsniveau zal eerst consensus moeten ontstaan alvorens de uiteindelijke oplossing(en) op haalbaarheid te kunnen beoordelen. Realisatietermijn is daarna het belangrijkste criterium, omdat de formulering van de opdracht was op te kijken naar de verschillende mogelijkheden op de korte termijn. Huidige dekkingsgraad is ook een graadmeter hiervoor.

De kansrijkheid van oplossingen zal vervolgens afhangen van andere aspecten. Hierbij zullen de criteria worden gehanteerd die door de branchevereniging voor webwinkeliers (Thuiswinkel.org) als belangrijkste werden genoemd: **'bereik** (huidige dekkingsgraad en schaalbaarheid) en **conversie** (begrijpbaarheid/gemak) tegen **acceptabele kosten** (businessmodel/betaalbaarheid)'. De criteria zijn op volgorde van prioriteit weergegeven in tabel 1.

---

<sup>7</sup> Onderzoek uitgevoerd door het ministerie van Veiligheid & Justitie. De geformuleerde criteria waren *Klantvriendelijk, Eenvoudig te communiceren* (samengevat in Begrijpbaarheid/Gemak), *Kostenbewust* (Businessmodel/betaalbaarheid), *Betrouwbaar* (Betrouwbaarheid), *Niet in strijd met privacywetgeving* (privacy / wetgeving), *Eenvormigheid* en *Implementatie* (Schaalbaarheid/flexibiliteit). Wij hebben deze nog aangevuld met 'Realisatietermijn' en 'Huidige dekkingsgraad' (als graadmeter voor realisatie op korte termijn conform de probleemstelling) en Beveiliging als randvoorwaarde naast wetgeving.

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	In hoeverre is de oplossing betrouwbaar voor webwinkeliers en klanten van de webwinkel. In hoeverre is de oplossing correct in het valideren van de leeftijd? Welke garanties biedt de oplossing?
Realisatietermijn	Wat is de tijd tot de realisatie en implementatie van de oplossing? Is de oplossing momenteel beschikbaar voor leeftijdsverificatie of moet de oplossing worden aangepast?
Huidige dekkingsgraad	Wordt de oplossing momenteel al ergens voor gebruikt en dan specifiek voor de verificatie van iemands leeftijd? Bijvoorbeeld: Nu al gebruikt voor betalingen, of als ID in een offline context.
Schaalbaarheid / Flexibiliteit	Is de oplossing ook inzetbaar voor andere toepassingen of in andere contexten? Bijvoorbeeld: Kunnen er naast de leeftijd ook bankgegevens worden geverifieerd, en is dit alleen mogelijk in een online context of ook via een mobiele telefoon?
Begrijpbaarheid / Gemak	Hoe makkelijk is de oplossing te begrijpen voor webwinkeliers en klanten van de webwinkel. Bijvoorbeeld: Moeten er handelingen worden verricht die evident zijn? In hoeverre is de oplossing eenvoudig te implementeren en te gebruiken voor de webwinkel? Hoe is het gebruiksgemak voor de klant?
Businessmodel / Betaalbaarheid	Wat zijn de aanvaardbare kosten per leeftijdsverificatie en de implementatiekosten voor de webwinkel?
Privacy / Wetgeving	Is de oplossing in lijn met de huidige wetgeving, moet er wetgeving worden aangepast om het mogelijk te maken of moet de oplossing worden aangepast? Specifiek gelet op de huidige wetgeving rondom privacy/bescherming persoonsgegevens.
Veiligheid	Hoe veilig is de oplossing? In hoeverre is de mogelijkheid tot identiteitsfraude en diefstal beperkt door het gebruik van de oplossing?

Tabel 1: Randvoorwaarden en succesfactoren voor online leeftijdsverificatie

## 5 Het aanbod van leeftijdsverificatiediensten

Er zijn verschillende oplossingen in de markt die zich presenteren als bruikbaar voor online leeftijdsverificatie. Ook zijn er diensten en systemen die, in aangepaste vorm, bruikbaar kunnen worden gemaakt voor leeftijdsverificatie op het web.

Dit hoofdstuk beschrijft de verschillende oplossingen op basis van de criteria uit paragraaf 4.4. Hoewel dit geen uitputtende lijst is, zijn deze (potentiële) oplossingen wel representatief voor de soorten identiteitsdiensten die op dit moment in Nederland en het omliggende buitenland in gebruik zijn.

### 5.1 CDDN



CDDN, Communicatie Data Diensten Nederland, is een bedrijf dat door middel van het delen van databestanden een oplossing biedt voor identiteitsvragen op internet. CDDN heeft een netwerk van partners die hun klantgegevens delen met het netwerk en zo samenwerken aan een basisbestand. Deze gegevens worden op bepaalde vaste ijkpunten gevalideerd door iedere maand te melden of een klant overleden is, verhuisd is en wanneer er voor het laatst contact is geweest op een adres met die klant.

Mogelijke oplossingen gaan verder dan alleen leeftijdsverificatie, omdat ook veel andere data gedeeld kan worden met het netwerk zoals fysieke adresgegevens of e-mailadressen. De gegevens die worden gedeeld in de database zijn naam, adres, telefoon, e-mailadres, geboortedatum, initialen, sekse (NATEGIS), aangevuld met wanneer er voor het laatst contact geweest is. Door deze data met verschillende aanbieders te vergelijken krijg je een betrouwbaar beeld van de persoon in de database. Daarbij wordt er binnen CDDN gedifferentieerd op betrouwbaarheid van de data, dat wil zeggen dat data van bepaalde partijen wordt beoordeeld op authenticiteit.

Momenteel zijn er 11,9 miljoen van de 12,6 miljoen Nederlandse volwassenen bekend in de gemeenschappelijke database van CDDN. Voor de personen onder de 18 kent de database momenteel een dekkingsgraad van tussen de 20 en 25 %. Deze gegevens zijn afkomstig van 362 bedrijven en hebben samen gezorgd voor 100 miljoen klant gegevens.

CDDN ziet de oplossing voor leeftijdsverificatie als volgt: een consument vult op de check-out pagina van de webwinkelier zijn gegevens in (naam, adres, geboortedatum). Vervolgens doet de webwinkelier een request bij CDDN voor een validatie van bepaalde gegevens, in dit geval de leeftijd. CDDN kan op dat moment teruggeven dat de ingevulde geboortedatum inderdaad klopt bij opgegeven naam en adres. CDDN heeft ook voorgesteld om dit

bijvoorbeeld in een stichting onder te brengen, die als trusted third party zou kunnen dienen.

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>- De oplossing is een check op een gemeenschappelijke database gevuld vanuit databases van bedrijven</li> <li>- De database is niet uitputtend, voornamelijk missen er gegevens van consumenten tussen de 16 en 18 jaar</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>- Op korte termijn beschikbaar</li> <li>- Verrijken van de database zal tijd nodig hebben, met name voor de categorie 16- tot 18-jarigen</li> </ul>
Huidige dekkingsgraad	<ul style="list-style-type: none"> <li>- 94,4% van de volwassen Nederlanders zijn bekend</li> <li>- De oplossing kent een verminderde dekkingsgraad voor consumenten tussen de 16 en 18 jaar</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>- Maakt gebruik van huidige infrastructuur, namelijk de database van CDDN</li> <li>- Inzetbaar voor meer dan alleen leeftijdsverificatie</li> <li>- Beschikbaar voor de mobiele telefoon</li> <li>- Integreerbaar met applicaties van de webwinkelier</li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>- Invullen van de persoonsgegevens op de website</li> <li>- Webwinkelier doet een request of de gegevens kloppen met de database van CDDN en krijgt response terug</li> </ul>
Businessmodel / Betaalbaarheid van leeftijdsverificatie	<ul style="list-style-type: none"> <li>- Ontwikkelkosten om de oplossing geschikt te maken voor leeftijdsverificatie alleen, nu krijgt de webwinkelier nog meerdere gegevens terug dan alleen of de persoon de leeftijd van 16 of 18 jaar heeft bereikt</li> <li>- Kosten per opvraag uit de database kunnen bij hoge volumes bedragen ongeveer €0,01</li> </ul>
Privacy / Wetgeving	<ul style="list-style-type: none"> <li>- Er moeten gegevens worden prijsgegeven aan de webwinkelier om de database te kunnen raadplegen, namelijk naam, adres, geboortedatum en evt. telefoonnummer, e-mailadres en sekse</li> <li>- Bedrijven kunnen alleen een check doen op de gegevens als zij deze klant ook in hun database hebben</li> </ul>
Veiligheid	<ul style="list-style-type: none"> <li>- De data is eigendom van de webwinkelier, daarom is CDDN alleen aansprakelijk als zij de data verkeerd teruggeven aan de webwinkelier</li> <li>- Er vindt geen daadwerkelijke authenticatie plaats, slechts verificatie van verstrekte gegevens. Identiteitsfraude is dus mogelijk als een minderjarige de gegevens van bijvoorbeeld een van de ouders invult</li> </ul>

Tabel 2: Randvoorwaarden en succesfactoren CDDN



## 5.2 DigiD<sup>8</sup>

DigiD is de huidige manier voor Nederlandse burgers om zich bij de overheid te identificeren via het online kanaal. De Belastingdienst werkt met DigiD en ook scholieren en studenten kunnen voor het regelen van hun studiezaken inloggen door middel van DigiD. Het DigiD platform is gebaseerd op het burger service nummer (BSN), dat wettelijk alleen gebruikt mag worden in een overheidscontext of voor de uitvoering van wettelijke taken.

Er zijn op dit moment geen plannen om DigiD voor leeftijdsverificatie of andere doeleinden beschikbaar te stellen aan webwinkeliers of andere commerciële partijen.

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	– De DigiD gegevens zijn gebaseerd op de GBA
Realisatietermijn	– De tijd om het te realiseren hangt af van de keuze van de overheid. Op dit moment zijn er geen plannen voor invoering ten behoeve van leeftijdsverificatie
Huidige dekkingsgraad <sup>9</sup>	– In 2011 waren er 9 miljoen DigiD gebruikersnamen uitgegeven
Schaalbaarheid / Flexibiliteit	– Er kan gebruik gemaakt worden van de huidige uitgegeven DigiD's – Potentieel inzetbaar voor meer dan leeftijdsverificatie, maar afhankelijk van de keuze van de overheid
Begrijpbaarheid / Gemak	– De consument moet inloggen met zijn DigiD, zoals hij dat nu al doet bijvoorbeeld op de site van de belastingdienst – De webwinkelier krijgt de gegevens door van een vertrouwde partij welke inzage heeft in de DigiD gegevens
Businessmodel / Betaalbaarheid van leeftijdsverificatie	– Er is geen businessmodel voor leveren van gegevens aan bedrijven
Privacy / Wetgeving	– Gebaseerd op het BSN, wat niet te gebruiken is voor private doeleinden
Veiligheid	– De huidige DigiD systemen worden regelmatig ge-audit en voldoen aan strenge Veiligheidseisen

Tabel 3: Randvoorwaarden en succesfactoren DigiD

<sup>8</sup> Het profiel van DigiD is opgesteld op basis van expertise van Innopay en publiek beschikbare bronnen. Er heeft geen interview plaatsgevonden met een vertegenwoordiger van DigiD.

<sup>9</sup> Informatie verkregen van Logius

### 5.3 eHerkenning

### eHerkenning

eHerkenning is een netwerkoplossing die het mogelijk maakt voor personen, werkzaam voor bedrijven, om deze bedrijven te vertegenwoordigen bij een overheidsdienstverlener.

Middelen worden uitgegeven op STORK niveau 1, 2, 3 of 4. Tegenwoordig is het mogelijk om ook bij niet overheidsdienstverleners een authenticatie uit te voeren. Het netwerk is volledig ingericht door marktpartijen. eHerkenning is dus zelf geen leverancier van de oplossing voor leeftijdsverificatie, maar een netwerk waar een leverancier van leeftijdendiensten gebruik van zou kunnen maken. Op dit moment is eHerkenning vooral gericht op authenticatie van bedrijven bij overheidsdienstverleners, maar functionaliteit die Business-to-business en Business-to-consumer transacties mogelijk maakt bestaat al en is vanaf 1 april 2013 live.

Een oplossing voor leeftijdsverificatie begint in de registratiefase waarbij het mogelijk is dat een gebruiker een eHerkenningmiddel aanvraagt bij een van de middeluitgevers in het netwerk. Dit middel kan op verschillende niveaus van betrouwbaarheid worden uitgegeven (gebaseerd op de STORK standaard). Vanaf STORK niveau 2 kunnen persoonsattributen zoals leeftijd worden vastgelegd. Vanaf STORK niveau 3 is er sprake van een fysiek uitgifteproces. Tijdens of na het uitgifteproces van het middel kunnen attributen zoals geboortedatum en leeftijd worden toegevoegd bij een middeluitgever, attributenregister of machtigingenregister. Bij de transactie kiest de relying party (in dit geval de webwinkelier) het betrouwbaarheidsniveau dat hij nodig acht voor zijn dienst en vraagt de benodigde attributen, in dit geval '16 jaar of ouder' of '18 jaar of ouder'. Omdat er wordt gewerkt met pseudoniemen ziet de webwinkelier geen informatie over de consument, maar alleen dat hij de leeftijd van 16/18 wel of niet heeft bereikt, in dit geval bv. '18 jaar of ouder' = true.

eHerkenning heeft al profielen voor attributen, en het is mogelijk om voor specifieke doelen aanvullende attributen te registreren. Vanaf 1 april 2013 komt met versie 1.5 van eHerkenning functionaliteit beschikbaar voor (leeftijds)verificatie van personen, die niet in het bezit zijn van een KVK nummer (business-to-consumer).

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>- eHerkenning is een afsprakenstelsel waarin de betrouwbaarheid met alle partijen in het netwerk wordt bewaakt, door onafhankelijke toetreding, certificering en toezicht</li> <li>- De webwinkelier kan het gewenste betrouwbaarheidsniveau kiezen voor de authenticatie</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>- Vanaf 1 april 2013 is eHerkenning bruikbaar voor consumenten zonder KvK nummer en dus beschikbaar voor leeftijdsverificatie</li> </ul>
Huidige dekingsgraad	<ul style="list-style-type: none"> <li>- Op dit moment alleen beschikbaar voor vertegenwoordigers van bedrijven met een KvK nummer</li> <li>- Vanaf 1 april 2013 (versie 1.5) kunnen ook personen zonder KVK nummer een middel aanvragen en wordt dienstverlening van bedrijven naar consumenten opgestart</li> <li>- Momenteel is de uitgifte van eHerkenningmiddelen beperkt tot minder dan 0,5% van de Nederlandse bevolking</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>- Brede ID-dienst door de generieke opzet van attributen. Het is bijvoorbeeld ook mogelijk om andere attributen vast te leggen, zoals adresgegevens, emailadressen, naam en geslacht.</li> </ul>
Businessmodel / Betaalbaarheid van leeftijdsverificatie	<ul style="list-style-type: none"> <li>- Bedrijven betalen voor de middelenuitgifte, de registratie van machtigen, en de voorzieningen, ook op transactie niveau. De relying party betaalt voor de aansluiting op het netwerk door een eHerkenningmakelaar.</li> <li>- Aanschaf van het middel ligt bij de gebruikers, prijzen verschillen afhankelijk van middelenuitgever en betrouwbaarheidsniveau</li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>- De consument logt in met zijn eHerkenningmiddel op de website van de webwinkelier</li> <li>- De Webwinkelier krijgt via het netwerk eHerkenning terug dat de consument de leeftijd van 16/18 heeft bereikt indien dit attribuut geregistreerd is bij of na uitgifte van het middel</li> </ul>
Privacy / Wetgeving	<ul style="list-style-type: none"> <li>- Er wordt alleen een pseudoniem doorgegeven samen met het attribuut dat aangeeft of de consument wel of niet ouder is dan 16 of 18</li> <li>- Consument bepaalt per transactie wat hij wil doorgeven</li> </ul>
Veiligheid	<ul style="list-style-type: none"> <li>- De Veiligheid van het systeem is vastgelegd in het afsprakenstelsel evenals de onafhankelijke toetredingscriteria en certificering</li> <li>- Deelnemers aan eHerkenning moeten een ISO 27001 certificering halen voor informatiebeveiliging</li> </ul>

Tabel 4: Randvoorwaarden en succesfactoren eHerkenning



## 5.4 eNIK/eRijbewijs

BZK is toekomstgericht en heeft onder andere in samenwerking met EZ een strategische verkenning in gang gezet om te onderzoeken of er naast DigiD ook andere mogelijkheden denkbaar zijn om de veiligheid en privacy van burgers, bedrijven en professionals blijvend te borgen met betrekking tot het verkrijgen van toegang tot de elektronische overheidsdienstverlening. Dit zou onder andere kunnen door middel van het ontwikkelen of beschikbaar krijgen van een eID authenticatiemiddel met het hoogste betrouwbaarheidsniveau (STORK level 4).

Eén van de vraagstukken van de verkenning is of de overheid verantwoordelijk is voor het ter beschikking stellen van authenticatiemiddelen voor tenminste digitale overheidsdienstverlening en of zij nieuwe eigen middelen zou moeten ontwikkelen. Een ander mogelijkheid is namelijk gebruik maken van marktmiddelen. Ook is van belang onder welke voorwaarden de ontwikkeling van deze middelen plaatsvindt. Deze middelen moeten bijvoorbeeld toekomstvast zijn, uitwisselbaar zijn voor toekomstige grensoverschrijdende dienstverlening tussen EU-lidstaten (een wens die voorkomt uit de Digitale Agenda van de Europese Commissie), veilig, betrouwbaar en vooral gebruiksvriendelijk zijn.

In de strategische verkenning zijn door BZK en EZ in samenwerking met medeoverheden en grote uitvoeringsorganisaties een aantal uitgangspunten voor een eID stelsel Nederland en eID authenticatiemiddelen voor burgers en bedrijven vastgesteld. Het gaat hierbij om governance en stelselafspraken tussen overheid en bedrijven.

Voor het eID authenticatiemiddel wordt in eerste instantie gedacht aan het plaatsen van de eID in een chip op een wettelijk identiteitsdocument (WID) zoals de Nederlandse identiteitskaart (eNIK) of het rijbewijs (eRijbewijs). Dit vereist echter aanpassing van bestaande wetgeving.

Ook worden de mogelijkheden verkend voor het plaatsen de eID op een niet-WID document en de toepassing van de mobiele telefoon als lezer en als drager. Dit vereist minder aanpassing van bestaande wetgeving, maar wellicht wel nieuwe wetgeving om (privacy)bescherming te borgen.

Met het eID authenticatiemiddel kan de burger zich voor digitale dienstverlening hoogwaardig (op het hoogste betrouwbaarheidsniveau) identificeren en authenticeren, een gekwalificeerde handtekening zetten onder een digitaal document en zijn/haar leeftijd online aantonen. Privacy by design is een belangrijk uitgangspunt: de claim 'ouder dan, jonger dan..' kan bewezen worden zonder dat er identificerende gegevens worden uitgewisseld. Het uitgangspunt is dat het eID authenticatiemiddel (eNIK/eRijbewijs) uiteindelijk voor zowel publieke als voor private digitale diensten te gebruiken is. Binnen de publieke dienstverlening wordt het BSN uitgewisseld, binnen de private dienstverlening alleen (sectorale)pseudoniemen, wederom om de privacy te borgen. Private partijen mogen namelijk het BSN niet gebruiken.

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>- De eNIK/eRijbewijs zal door de overheid worden uitgegeven op basis van de gegevens in de GBA</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>- Het duurt minimaal nog 2 jaar voordat de wetgeving is aangepast en aanbestedingen zijn afgerond om het gebruik van de eNIK/eRijbewijs mogelijk te maken</li> </ul>
Huidige dekkingsgraad	<ul style="list-style-type: none"> <li>- De chip/eID is nog niet opgenomen op de NIK of rijbewijs, dus er zijn op dit moment ook geen eNIKS in omloop</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>- Alle bestaande NIK's en rijbewijzen moeten worden vervangen en/of nieuwe NIK's/rijbewijzen moeten worden uitgegeven.</li> <li>- Inzetbaar voor meer dan leeftijdsverificatie alleen, bijvoorbeeld attributen die nu ook op een wettelijk identiteit document (WID) staan, is denkbaar.</li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>- De kaart kan met behulp van een smartcardreader in een online context gebruikt worden (mobiele telefoon als drager is nog in onderzoek)</li> <li>- Webwinkelier doet een request of de opgegeven leeftijd klopt met de gegevens op de kaart (vlgs. het hit/no hit principe)</li> </ul>
Businessmodel / Betaalbaarheid van leeftijdsverificatie	<ul style="list-style-type: none"> <li>- Kosten voor de consument bij uitgifte niet per definitie gratis</li> </ul>
Privacy / Wetgeving	<ul style="list-style-type: none"> <li>- De webwinkelier krijgt alleen een 'privacy by design' antwoord terug, dus alleen of de consument wel of niet boven de 16 of 18 is</li> <li>- Aan de hand van doelbinding mag je uitvragen wat je nodig acht voor het leveren van het product of de dienst (doelbinding, dataminimalisatie, zelfbeschikking door de burger)</li> </ul>
Veiligheid	<ul style="list-style-type: none"> <li>- Gebaseerd op STORK 4/PKIoverheid voor zeer veilige digitale certificaten uitgegeven door gecertificeerde partijen</li> </ul>

Tabel 5: Randvoorwaarden en succesfactoren eNIK/eRijbewijs

## 5.5 Experian



Experian is een informatieleverancier voor het leveren van data en analytische instrumenten aan klanten wereldwijd. Het bedrijf helpt ondernemingen om kredietrisico's te beheersen, fraude te voorkomen, marketinginstrumenten gericht in te zetten en de besluitvorming te automatiseren. Daarnaast helpt Experian ook consumenten met het verschaffen van inzicht in hun kredietwaardigheid en credit score, en door hen te beschermen tegen identiteitsfraude (bijvoorbeeld d.m.v. leeftijdscompliance).

Experian is een bedrijf dat zich sinds 1986 in Nederland heeft gespecialiseerd in het verkrijgen van databronnen en databanken om een zo duidelijk mogelijk beeld te vormen van consumenten. Grote databanken van bekende partijen, zoals het Kadaster, de Kamer van Koophandel en de grote telefoonaanbieders, zijn samengevoegd in de databanken van Experian. Veel van de klanten van Experian maken gebruik van de producten onder reciprociteit, en leveren zo hun positieve en negatieve betalingservaringen met consumenten aan Experian. In het buitenland heeft Experian veel ervaring met officiële personenregisters, bijvoorbeeld het centrale kredietregistratiesysteem van het Verenigd Koninkrijk en Denemarken (vergelijkbaar met het BKR en GBA hier).

Voor de e-commerce markt is er een oplossing ontwikkeld waarmee real-time de e-identity van de klant, frauderisico's (oa leeftijd) én kredietwaardigheid worden gecheckt.

Het product dat Experian aanbiedt gaat verder dan alleen leeftijdsverificatie, het is namelijk ook mogelijk om adressen te verifiëren en de kredietwaardigheid van consumenten te controleren. Experian schat ongeveer 86% van de economisch actieve Nederlanders boven de achttien te kunnen identificeren op naam en adres.

De oplossing voor leeftijdsverificatie van Experian werkt als volgt: een consument komt op de check-out pagina van de webwinkelier en vult zijn gegevens in. De webwinkelier doet bij Experian een real-time check of deze gegevens kloppen met de database van Experian.

Experian levert dan een aantal gegevens terug die inzicht geven in de waarschijnlijkheid dat de persoon zijn rekening zal betalen en de waarschijnlijkheid dat een persoon is wie hij aangeeft te zijn. Onderdeel van het product is een 16+ en een 18+ validatie.

Dit wordt onder andere gedaan door te verifiëren of de combinatie (geheel of gedeeltelijk) van naam, initialen, geboortedatum en adresgegevens bekend zijn. Ook wordt er onder andere gevalideerd of de naam überhaupt in Nederland voorkomt en of het adres bestaat. Dit betreft een bestaande applicatie die Experian aanbiedt onder de naam E-commerce Check.

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>- De oplossing bestaat uit een check op een beheerde databank in combinatie met scorekaart</li> <li>- De database is niet uitputtend, de oplossing kent een verminderde dekkingsgraad tussen de 16 en 23 jaar</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>- Beschikbaar</li> <li>- Verrijken van de database met gegevens van 16- tot 18-jarigen zal tijd nodig hebben; Experian onderzoekt mogelijkheden om met afgeleide data een oplossing te realiseren</li> </ul>

Huidige dekkingsgraad	<ul style="list-style-type: none"> <li>- 86% van alle Nederlanders die aan e-commerce doen zijn bekend</li> <li>- De oplossing kent een verminderde dekkingsgraad tussen de 16 en 23 jaar</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>- Maakt gebruik van huidige infrastructuur, namelijk de database van Experian</li> <li>- Beschikbaar voor meer dan alleen leeftijdsverificatie</li> <li>- Experian overweegt een App te bouwen</li> <li>- Integreerbaar met applicaties van de webwinkelier (XML/SOAP)</li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>- Invullen van de persoonsgegevens op de website</li> <li>- Webwinkelier doet een request naar de gegevens die bekend zijn in de database van Experian</li> </ul>
Businessmodel / Betaalbaarheid van leeftijdsverificatie	<ul style="list-style-type: none"> <li>- Kosten per opvraag uit de database kunnen bij hoge volumes tegen een laag tarief worden aangeboden</li> </ul>
Privacy / Wetgeving	<ul style="list-style-type: none"> <li>- Experian Nederland is aangesloten bij de Nederlandse Vereniging van Handelsinformatiebureaus (NVH) en werkt conform de Wet Bescherming Persoonsgegevens</li> <li>- Er moeten gegevens worden prijsgegevens aan de webwinkelier om de database te kunnen raadplegen. Experian screent haar klanten zorgvuldig alvorens hen toegang te geven tot haar producten</li> <li>- Experian kan teruggeven aan de webwinkelier dat de persoon 16/18 is, zonder overige informatie terug te geven</li> <li>- Bedrijven die gebruik maken van de service moeten een contract afsluiten met Experian waarin ze aangeven zorgvuldig om te gaan met de data</li> </ul>
Veiligheid	<ul style="list-style-type: none"> <li>- Experian vervult alleen een adviesrol, de verantwoordelijkheid om een zakelijke relatie aan te gaan zal blijven liggen bij de webwinkelier</li> <li>- Er vindt geen daadwerkelijke authenticatie plaats, slechts verificatie van verstrekte gegevens. Identiteitsfraude is dus mogelijk als een minderjarige de gegevens van bijvoorbeeld een van zijn ouders invult</li> </ul>

Tabel 6: Randvoorwaarden en succesfactoren Experian

## 5.6 IDchecker



IDchecker levert, een brede dienst voor ID verificatie via het online kanaal. De oplossing, welke live is vanaf april 2005, is gebaseerd op OCR, optical character recognition. De consument maakt een digitale afbeelding van zijn identiteitsdocument (paspoort, rijbewijs, identiteitskaart), of toont zijn document voor de webcam van zijn computer, waarna deze afbeelding beveiligd wordt verstuurd aan de servers van IDchecker. IDchecker kent verschillende soorten pakketten welke worden aangeboden aan de klant, variërend van geautomatiseerde check op echtheidskenmerken, een computer check op de MRZ (machine readable zone) code, tot het bestuderen van het document op vervalsing door een documentenexpert. Er kan worden gekeken of het document bekend is in een database voor

gestolen ID documenten en. Het is mogelijk om de oplossing rechtstreeks te integreren in de website van de webwinkelier. De webwinkelier krijgt dan een afbeelding van het document te zien in zijn back-end systeem. Zo kan hij de leeftijd van de klant verifiëren. Het is ook mogelijk om IDchecker als tussenpersoon te laten fungeren, die alleen aan de webwinkelier terug geeft of de consument ouder is dan 16/18 jaar. In dit laatste geval hoeft niet de afbeelding van het WID document naar de webwinkelier te worden gestuurd. IDchecker treedt op dat moment op als een trusted third party. Deze oplossingsvariant is volgens IDchecker eenvoudig te realiseren en voldoet aan Wet Bescherming Persoonsgegevens.

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>- Elk document dat gescand wordt, wordt gecontroleerd op echtheidskenmerken</li> <li>- Mogelijk om een documentenexpert naar document te laten kijken</li> <li>- Validatiecheck heeft betrekking op het document, niet op de persoon</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>- Direct beschikbaar</li> </ul>
Huidige dekkinggraad	<ul style="list-style-type: none"> <li>- Iedereen die in het bezit is van een Nederlands WID document: Paspoort, rijbewijs, ID-Kaart en ook mogelijk voor 213 landen en ruim 3500 typen documenten</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>- Maakt gebruik van huidige infrastructuur (mits een webcam of scanner beschikbaar is) en ID documenten</li> <li>- Oplossing is uit te breiden naar andere identiteitskenmerken mits die op het WID document staan</li> <li>- Beschikbaar voor de mobiele telefoon</li> <li>- IDchecker heeft eigen mobiele app, maar de dienst is ook integreerbaar met apps van bijvoorbeeld webwinkeliers</li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>- Presenteren van een WID document voor een webcam of digitaliseren met een mobile app of reguliere scanner</li> <li>- Webwinkelier ziet gegevens van het WID document, net zoals bij tonen (kopie van) WID document in de offline wereld</li> </ul>
Businessmodel / Betaalbaarheid van leeftijdsverificatie	<ul style="list-style-type: none"> <li>- Product is geschikt om ID bewijzen te controleren op Nederlandse markt</li> <li>- Kosten per scan variëren op basis van de aantallen tussen ongeveer rond de € 0,40 en € 0,50 voor de Basis Check</li> <li>- Hoe de kosten per verificatie verdeeld worden ligt aan hoe het eindproduct zal worden ingericht</li> </ul>
Privacy / Wetgeving	<ul style="list-style-type: none"> <li>- Compliant te maken aan (de Nederlandse) wetgeving</li> <li>- ID document moet gescand worden door de koper en scan wordt opgeslagen door verkoper, of door IDchecker</li> </ul>

Veiligheid	<ul style="list-style-type: none"> <li>- IDchecker is juridisch gezien een bewerker, wat inhoudt dat er geen aansprakelijkheid geaccepteerd wordt bij een vervalst document. Bij de Full Check is er wel een mogelijkheid om het risico over te nemen.</li> <li>- Het is niet standaard nodig om ook het gezicht van de consument te tonen bij het identiteitsbewijs. Fraude door het tonen van het WID document van iemand anders is daarmee een mogelijkheid</li> </ul>
------------	---

Tabel 7: Randvoorwaarden en succesfactoren IDchecker

## 5.7 iDEAL



iDEAL is een oplossing die bekend is van het online betalen. In beginsel is iDEAL geschikt te maken voor leeftijdsverificatie en andere e-identity diensten door de beheerorganisatie Currence. Voor een daadwerkelijke implementatie door de licentiehouders moeten zij bovendien hun klantgegevens beschikbaar maken voor deze e-identity diensten zoals leeftijdsverificatie. Een iDEAL-gebaseerde oplossing voor leeftijdsverificatie zou kunnen werken op eenzelfde manier zoals iDEAL nu werkt voor het doen van een online betaling. Tijdens de transactie geeft de consument toestemming om ook zijn persoonsgegevens (in dit geval leeftijd) op te vragen bij zijn bank, waarna de consument wordt doorgeleid naar de bank om zich te identificeren op de gebruikelijke manier (e-identificatie, TAN-code, etc). Na een geslaagde authenticatie wordt de klant teruggeleid naar de website van de webwinkelier en ontvangt de webwinkelier naast de betaalbevestiging de gevraagde leeftijdsgegevens. Het is op deze manier alleen mogelijk om te laten weten of de klant 16/18 jaar is.

De iDEAL standaard kan hiervoor geschikt gemaakt worden door iDEAL-berichten aan te passen aan het gebruik in e-identity diensten. Vervolgens zouden banken deze functionaliteit dan moeten inbouwen in hun iDEAL systemen en deze aansluiten op hun database met klantgegevens. Het is de verwachting dat een dergelijke aanpassing in ieder geval zal moeten wachten tot na het nu lopende traject om iDEAL geschikt te maken voor SEPA (de Single Euro Payment Area).

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>- iDEAL wordt al gebruikt voor online betalen</li> <li>- Banken en iDEAL hebben een betrouwbaar imago en banken beschikken over geverifieerde klantgegevens</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>- Er is geen plan bij Currence om iDEAL te voorzien van leeftijdsfunctionaliteit</li> <li>- Er is geen vraag bij licentiehouders van iDEAL om leeftijdsfunctionaliteit toe te voegen</li> <li>- Het aanpassen van de standaard en doorvoeren van de veranderingen bij</li> </ul>

	de licentiehouders duurt naar verwachting minimaal 1 tot 2 jaar, zelfs als nu een dergelijk besluit wordt genomen
Huidige dekkingsgraad	<ul style="list-style-type: none"> <li>- Alle consumenten die nu een contract hebben voor internetbankieren kunnen gebruik maken van iDEAL</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>- Er wordt gebruikt gemaakt van de huidige infrastructuur voor online bankieren</li> <li>- Inzetbaar voor meer dan leeftijdsverificatie, met potentieel alle attributen die bekend zijn voor een klant bij zijn bank</li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>- De consument doet een online betaling met iDEAL en in dezelfde transactie wordt de leeftijd geverifieerd.</li> <li>- De consument rondt de transactie af op dezelfde manier als hij gewend is van iDEAL betalingen</li> </ul>
Businessmodel / Betaalbaarheid van leeftijdsverificatie	<ul style="list-style-type: none"> <li>- De kosten per transactie zijn in dit stadium nog niet bekend.</li> </ul>
Privacy / Wetgeving	<ul style="list-style-type: none"> <li>- De webwinkelier krijgt alleen een 'privacy by design' antwoord terug, dus alleen of de consument wel of niet boven de 16 of 18 is</li> <li>- Bank moet nieuwe voorwaarden afspreken met de consument om andere gegevens door te kunnen geven via de iDEAL betaling</li> </ul>
Veiligheid	<ul style="list-style-type: none"> <li>- iDEAL is een bekend systeem dat al jaren gebruikt wordt voor betalingen op basis van online bankieren en gebruik maakt van digitale certificaten voor beveiligen van de verbindingen en berichten</li> </ul>

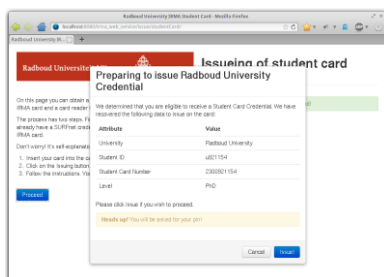
Tabel 8: Randvoorwaarden en succesfactoren iDEAL

## 5.8 IRMA

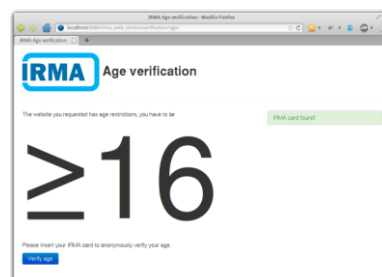


De Radboud Universiteit Nijmegen werkt samen met TNO en SURFnet aan een oplossing voor attribootgebaseerde (online) verificatie (binnen het kader van het Privacy and Identity Lab). Het project voor de IRMA (I Reveal My Attributes) kaart, is een half jaar geleden opgestart, maar er is al meerdere jaren onderzoek gedaan naar deze oplossing. De oplossing is gebaseerd op een persoonsgebonden chipkaart waarbij attributen (naam, leeftijd, adres, boven de 18 ja/nee, student ja/nee, etc.) in de chip kunnen worden geladen door de gebruiker. Deze attributen kunnen los van elkaar getoond worden. Met cryptografische technieken wordt de veiligheid en echtheid van de data gewaarborgd. De techniek die gebruikt wordt heet Idemix (Identity Mixer). Dit is een verzameling van cryptografische protocollen die er voor zorgt dat de privacy van de consument beschermd wordt. De IRMA

smartcard toont aan de buitenkant alleen een foto van de gebruiker en echtheidskenmerken van de kaart. In de toekomst zou de kaart op bepaalde punten geladen kunnen worden met gegevens. Te denken valt aan de website mijnoverheid.nl en andere partners die samenwerken met IRMA. Naast identiteitsattributen valt ook te denken aan coupons of waardepunten van winkels, aan een rol-beschrijving (arts, verpleger), of aan een micro-epd, of aan toegangsrechten. De kaarteigenaar accepteert bij verificatie de voorwaarden en kan aangeven met een pincode dat hij gegevens op zijn kaart geladen wil hebben. Deze smartcard uitlezen duurt 1-2 seconden en kan worden gedaan via een smartcard reader of contactloos via Near Field Communicatie (NFC) technologie op smart phones en tables. Het is ook mogelijk om je eigen kaart uit te lezen met je eigen persoonlijke pincode om te allen tijden te controleren wat er op de kaart staat. De kaart is bruikbaar in zowel een online als een offline context. Bruikbaarheid is vooral afhankelijk van het aantal partners waarbij gegevens op de kaart geladen kunnen worden en het betrouwbaarheidsniveau van de gegevens die op de kaart worden geladen (uitgifteproces). Bij online leeftijdsverificatie vraagt de (web)winkelier of de consument kenbaar wil maken of hij ouder is dan 16/18 jaar. De consument geeft aan dat hij dit wil door zijn IRMA kaart in de cardreader te stoppen of door de NFC technologie te activeren.



Figuur 5: Uitgifte proces van een studentenattribuut



Figuur 6: Voorbeeld leeftijdsverificatie check

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>De oplossing is een check op de IRMA kaart, welke gebruikt maakt van cryptografische technieken (Idemix)</li> <li>De betrouwbaarheid van de attributen hangt af van de mate waarin ze door vertrouwde partijen worden uitgegeven</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>In het tweede kwartaal van 2013 wordt verwacht dat er een grootschalige proef mogelijk is met de oplossing</li> </ul>
Huidige dekkingsgraad	<ul style="list-style-type: none"> <li>Er zal gebruik worden gemaakt van bestaande databases</li> <li>De IRMA kaarten moeten nog worden uitgegeven, er is geen huidige dekking</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>Er moeten nieuwe kaarten worden uitgegeven aan een groot deel van de Nederlanders</li> <li>Te gebruiken op de computer en andere mobiele apparaten (mits voorzien</li> </ul>



	<ul style="list-style-type: none"> <li>van smartcard reader of NFC) <ul style="list-style-type: none"> <li>– Ook inzetbaar in de offline context</li> <li>– Inzetbaar voor meer dan alleen leeftijdsverificatie</li> </ul> </li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>– De kaart moet gebruikt worden in een smartcard reader of via de NFC functie van bijvoorbeeld een telefoon/tablet</li> <li>– Webwinkelier controleert of de gegevens kloppen met de gegevens op de kaart</li> </ul>
Businessmodel / Betaalbaarheid van leeftijdsverificatie	<ul style="list-style-type: none"> <li>– De chip kost € 1 maar het uitgifteproces van de kaarten zou kunnen oplopen tot € 10, wat te vergelijken is met de OV chipkaart</li> <li>– Verificaties zijn gratis indien door de winkelier zelf uitgevoerd; bij uitbesteding zal het verificatieproces niet kostenloos zijn</li> </ul>
Privacy / Wetgeving	<ul style="list-style-type: none"> <li>– De consument beslist zelf welke attributen hij op zijn IRMA kaart laadt en toont aan de (web)winkelier</li> <li>– De (web)winkelier krijgt alleen een antwoord terug als de consument hiervoor toestemming geeft. De (web)winkelier krijgt alleen te zien of de consument de leeftijd van 16 of 18 jaar heeft bereikt</li> </ul>
Veiligheid	<ul style="list-style-type: none"> <li>– Gebaseerd op cryptografische technieken die al 10 jaar bekend zijn in de wetenschappelijke literatuur, zorgt voor hoge betrouwbaarheid en sterke technische bescherming van de vertrouwelijke gegevens</li> </ul>

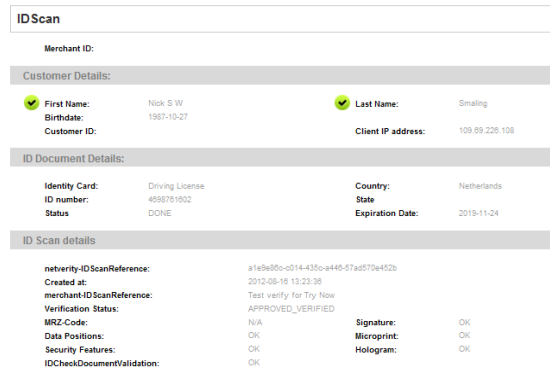
Tabel 9: Randvoorwaarden en succesfactoren IRMA

## 5.9 Jumio



Jumio biedt een oplossing genaamd Netverify, een brede dienst voor ID verificatie via het online en mobiele kanaal. De oplossing is gebaseerd op OCR, Optical Character Recognition. Een consument biedt zijn identiteitsdocument (paspoort, rijbewijs of ID-kaart) aan voor de webcam van zijn computer, of maakt een digitale afbeelding van zijn ID bewijs, waarna deze via een beveiligd kanaal wordt verstuurd aan de servers van Jumio. Het is mogelijk om de verbinding naar Jumio te integreren via een iFrame op de website van de webwinkelier. Mocht het nodig zijn dan is Netverify in staat om de MRZ (machine readable zone) code te lezen van het document. Het is mogelijk om de hologrammen en overige echtheidskenmerken te verifiëren om de echtheid van het document vast te stellen. Verder kan worden gekeken of het document bekend is in een database voor gestolen ID documenten en kan worden gecontroleerd waar het IP-adres van de consument geregistreerd staat. De webwinkelier krijgt een kopie van het document te zien in zijn beheerpagina waar hij de geboortedatum op kan aflezen en zo de leeftijd van de klant kan verifiëren. Het is eventueel mogelijk om dit proces te automatiseren. Jumio heeft aangegeven ook open te staan voor een trusted third party aanpak, waarbij de gegevens van het ID document alleen worden verstuurd aan een intermediair, die de leeftijdscheck uitvoert en alleen doorgeeft dat de persoon ouder of jonger is dan 16/18 jaar. Een dergelijke oplossing voldoet beter aan de Wet Bescherming Persoonsgegevens omdat er geen kopie

van het WID document wordt doorgegeven aan de webwinkelier. Dit is momenteel nog niet operationeel, maar Jumio heeft aangegeven te willen meewerken aan een oplossing en staat positief tegenover opzetten van een proof of concept.



Figuur 7: Document scan via de webcam voor de gebruiker

Figuur 8: Back-end van de webwinkelier ziet de volgende gegevens

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>– Elk document dat gescand wordt, wordt gecontroleerd op echtheidskenmerken</li> <li>– Validatie check heeft betrekking op het document, niet op de persoon</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>– Het is beschikbaar, maar zal moeten worden aangepast aan Nederlandse wetgeving.</li> <li>– 3-6 maanden is geschatte realisatietermijn voor doorvoeren van de benodigde wijzigingen, inclusief testen</li> </ul>
Huidige dekingsgraad	<ul style="list-style-type: none"> <li>– Iedereen die in het bezit is van een Nederlands WID document: Paspoort, rijbewijs, ID-Kaart</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>– Maakt gebruik van huidige infrastructuur (mits een webcam of scanner beschikbaar zijn) en ID documenten</li> <li>– Oplossing is uit te breiden naar andere identiteitskenmerken mits die op het WID document staan</li> <li>– Vanaf eind 2012 ook beschikbaar voor de mobiele telefoon (&gt;3MP camera)</li> <li>– Jumio heeft een eigen mobiele app, maar de dienst is ook integreerbaar met apps van bijvoorbeeld webwinkeliers</li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>– Presenteren van ID kaart voor een webcam</li> <li>– Webwinkelier ziet ID kaart, net zoals in een offline wereld</li> </ul>
Businessmodel / Betaalbaarheid	<ul style="list-style-type: none"> <li>– Kosten per scan variëren op basis van de aantallen tussen de 1 en 2 euro</li> <li>– Hoe de kosten per verificatie verdeeld worden ligt aan hoe het eindproduct</li> </ul>

	zal worden ingericht
Privacy / Wetgeving	<ul style="list-style-type: none"> <li>- In de VS al volledig compliant aan lokale wetgeving</li> <li>- ID document moet gescand worden door de koper en scan wordt opgeslagen door verkoper</li> </ul>
Veiligheid	<ul style="list-style-type: none"> <li>- Jumio aanvaardt geen aansprakelijkheid voor de geleden schade bij onjuiste verificatie</li> <li>- Het is niet standaard nodig om ook het gezicht van de consument te tonen bij het identiteitsbewijs. Fraude door het tonen van het WID document van iemand anders is daarmee een mogelijkheid. Gezichtsherkenning is mogelijk in Q1 van 2013.</li> </ul>

Tabel 10: Randvoorwaarden en succesfactoren Jumio

## 5.10 KPN



KPN is al een tijd bezig om na denken over de rollen en business cases van het bedrijf gezien de opkomst van datagedreven telefonie. Op dit moment is KPN bezig om te kijken hoe ze hun rol in het Nederlandse e-identity landschap kunnen spelen. KPN bezit een rijke database aan klantgegevens welke voor verschillende doeleinden zou kunnen worden ingezet. Ook speelt het leeftijdsverificatie vraagstuk hier een rol. Leefijdsverificatie wordt gezien als onderdeel van de e-identity agenda en daarvan zijn de tijdlijnen op dit moment niet bekend.

## 5.11 PostNL



PostNL vult al een markt vraag in naar validatieservices voor persoons- of persoonsgerelateerde kenmerken en constateert dat er een markt vraag is naar leeftijdsverificatie binnen een online context. Vanuit overheid en diverse branches wordt PostNL benaderd om een maatschappelijke rol te vervullen op het vlak van identificatie en verificatie voor leeftijdsgebonden diensten.

PostNL heeft hiervoor een aantal competenties, welke haar in staat stellen hieraan te voldoen, o.a. een betrouwbaar en herkenbaar merk, databronnen met zakelijke en consumentengegevens, een netwerk fysieke identificatie (balies en aan de deur) en bestaande oplossingen & markt bereik.

PostNL biedt momenteel offline verificatie van identiteiten (incl. leeftijd) zowel aan 2600 PostNL balies als op de locatie van de consument (thuis, kantoor).

Daarnaast is PostNL betrokken bij een initiatief dat online leeftijdsverificatie gemakkelijk, secure en met bescherming van privacy ontwikkelt. Het initiatief, i.s.m. enkele andere Nederlandse marktpartijen, maakt het mogelijk vele soorten gegevens tegen verschillende betrouwbare databronnen (zoals GBA) te verifiëren en direct toepasbaar te maken voor verschillende (markt) behoeftes. Hieronder valt verificatie van leeftijd, die toepasbaar is in bijvoorbeeld bescherming van ‘adult content’, online drankverkoop en gaming. Hiervoor is het noodzakelijk om toegang te krijgen tot deze databronnen, om deze te kunnen gebruiken voor verificatie.

PostNL kan (leeftijds-)verificatie uitvoeren op verschillende betrouwbaarheidsniveaus. Een combinatie van het ontsluiten van databronnen en verificatie op een fysieke locatie van PostNL behoort tot de mogelijkheden. Fysieke identificatie in een online context is voor PostNL een belangrijk speerpunt om het gemak van online te combineren met de betrouwbaarheid van Post, om behoefte aan online veilig zakendoen in te vullen.

RANDVOORWAARDEN / SUCCESFACTOREN	BESCHRIJVING
Betrouwbaarheid	<ul style="list-style-type: none"> <li>- De oplossing vergelijkt gegevens met een geverifieerde database</li> <li>- De betrouwbaarheid van de oplossing is aan te passen op de behoefte. E.g. voor de ene toepassing van de online leeftijdscheck is een lager betrouwbaarheidsniveau nodig dan voor een andere</li> </ul>
Realisatietermijn	<ul style="list-style-type: none"> <li>- Realisatie Q2 2013, mits databronnen beschikbaar</li> <li>- Tussentijds kan leeftijdsverificatie via de huidige oplossing van PostNL plaatsvinden (controle aan de deur), maar deze heeft hoge kosten en is alleen bruikbaar voor fysieke levering van goederen</li> </ul>
Huidige dekkingsgraad	<ul style="list-style-type: none"> <li>- Er wordt gebruik gemaakt van bestaande databases, waarmee in principe 100% dekkingsgraad te realiseren is</li> <li>- Consumenten kunnen langs gaan om hun data te laten valideren en om een e-ID middel aan te maken bij een locatie van PostNL</li> </ul>
Schaalbaarheid / Flexibiliteit	<ul style="list-style-type: none"> <li>- Inzetbaar voor meer dan alleen leeftijdsverificatie</li> </ul>
Begrijpbaarheid / Gemak	<ul style="list-style-type: none"> <li>- Online, directe verificatie van leeftijd</li> <li>- Inloggen met een e-ID dat de consument/ burger al in bezig heeft of eenvoudig kan verkrijgen, bijv. op een locatie van PostNL</li> </ul>
Businessmodel / Betaalbaarheid van leeftijdsverificatie	<ul style="list-style-type: none"> <li>- Er zijn verschillende, nog nader te onderzoeken, businessmodellen mogelijk</li> </ul>

Privacy / Wetgeving	<ul style="list-style-type: none"> <li>- De website krijgt alleen een antwoord op de gestelde vraag terug, dus alleen of de consument wel of niet boven de 16 of 18 is</li> <li>- De consument kiest zelf voor de bron waar zijn/haar leeftijd geverifieerd wordt</li> <li>- De bron krijgt niet te weten waarvoor de leeftijdsverificatie wordt gebruikt</li> </ul>
Veiligheid	<ul style="list-style-type: none"> <li>- De kans op identiteitsfraude hangt af van de toegepaste authenticatie, die te kiezen is door de dienstverlener</li> </ul>

Tabel 11: Randvoorwaarden en succesfactoren PostNL

## 5.12 Banken

Banken kunnen ook een rol kunnen spelen in het e-identity landschap met betrekking tot leeftijdsverificatie. Zij bezitten immers de informatie welke relevant is voor het uitvoeren van leeftijdsverificatie en worden in de maatschappij (nog steeds) gezien als een vertrouwde instelling. Bij verschillende banken is de vraag uitgezet of zij interesse hadden om mee te werken naar een marktverkenning voor online leeftijdsverificatie in Nederland. De reacties geven aan dat men het onderwerp herkent, maar er nu niet actief mee bezig is.

Dit werd bevestigd door De Nederlandse Vereniging van Banken (NVB) die aangeeft dat banken jaren terug betrokken zijn geweest, in verband met het mogelijk aanbrenge van een leeftijdsindicator in de chipknip. Dit zou als oplossing ingezet kunnen worden bij sigarettenautomaten maar is uiteindelijk niet ingevoerd. Op dit moment zien banken geen aanleiding om iets specifiek met leeftijdsverificatie te doen. Leeftijdsverificatie wordt gezien als onderdeel van de e-identity agenda en daarvan zijn de tijdlijnen op dit moment niet bekend. Specifieke bankenoplossingen (los van iDEAL) zijn daarom verder niet bekeken.

## 6 Analyse

De elf potentiële oplossingen zijn met elkaar vergeleken op basis van de in paragraaf 4.4 geprioriteerde randvoorwaarden en succesfactoren. Allereerst worden de individuele criteria besproken, waarna er een ranking van oplossingen wordt gepresenteerd.

### 6.1 Betrouwbaarheid

Het criterium betrouwbaarheid geeft aan in hoeverre de oplossing betrouwbare informatie biedt voor webwinkeliers. Cruciaal hier is met welke mate van zekerheid de oplossing correct is in het valideren van de leeftijd van de consument. Voor dit criterium is een onderscheid te maken in de drie niveaus beschreven in paragraaf 3.1.

Op Niveau 1 bevinden zich de oplossingen die gebruik maken van datavalidatie tegen een (externe) database. Deze groep omvat de oplossingen van **CDDN, Experian, KPN** en **PostNL** (bij controle tegen externe databases). Hierbij worden de ingevulde persoonsgegevens van de consument vergeleken met één of meer databases op basis waarvan met een bepaalde zekerheid kan worden aangenomen dat de consument ook daadwerkelijke de persoon is die hij claimt te zijn.

Bij datavalidatie oplossingen zou het kunnen gebeuren dat iemand de gegevens van een andere persoon invult, bijvoorbeeld van één van de ouders, en op die manier het systeem om de tuin leidt omdat de ouders op het zelfde adres wonen en de vereiste leeftijd hebben. Dit is een vorm van *'family fraud'* en is bij dit soort systemen moeilijk uit te sluiten omdat er geen sprake is van een geheim (bijvoorbeeld wachtwoord of pincode) dat de gebruiker uniek identificeert. Overigens kan *family fraud* ook bij afgeleide of directe identificatie optreden indien familieleden toegang hebben tot elkaars inlogcodes, pincodes of pasjes.

Een ander mogelijk manco in de betrouwbaarheid van datavalidatie is dat de databases die gebruikt worden niet noodzakelijk gebaseerd hoeven te zijn op een authentieke bron zoals de GBA. Het niveau van betrouwbaarheid van de bron speelt ook bij afgeleide identificatie een rol: hier is vooral van belang of er in het proces van uitgifte van een authenticatiemiddel een (betrouwbare) controle van een wettelijk ID bewijs heeft plaatsgevonden. Een bankpas gebruikt voor iDEAL (alleen uitgereikt na tonen van ID bewijs) is hierin dus betrouwbaarder dan een DigiD (waarvan de code wordt verstuurd naar het huisadres zoals bekend in de GBA).

Binnen de categorie van datavalidatie vallen ook de oplossingen van **IDchecker** en **Jumio**. Hoewel het bij deze systemen lijkt te gaan om directe controle van een wettelijk identiteitsbewijs, wordt in werkelijkheid niet gecontroleerd of het getoonde identiteitsbewijs daadwerkelijk behoort bij de consument die het toont. Het betreft hier dus

alleen de validatie van de gegevens op het getoonde ID bewijs zelf (mogelijk aangevuld met een check of het document niet als gestolen aangemerkt is). Hoewel het dus meer zekerheid geeft dan validatie puur op basis van ingevulde persoonsgegevens door een consument, heeft het hetzelfde manco als andere validatiemethodes met betrekking tot *family fraud*.

Oplossingen van Niveau 2 doen daadwerkelijk een real-time authenticatie van de consument, gebaseerd op een eerdere controle van een wettelijke identiteit. Binnen deze categorie vallen **DigiD**, **eHerkenning**, **iDEAL**, **IRMA** en **PostNL** (bij gebruik van een gevalideerde e-ID). De risico's rond *family fraud* en de afhankelijkheid van een betrouwbaar uitgifteproces zijn hierboven al beschreven.

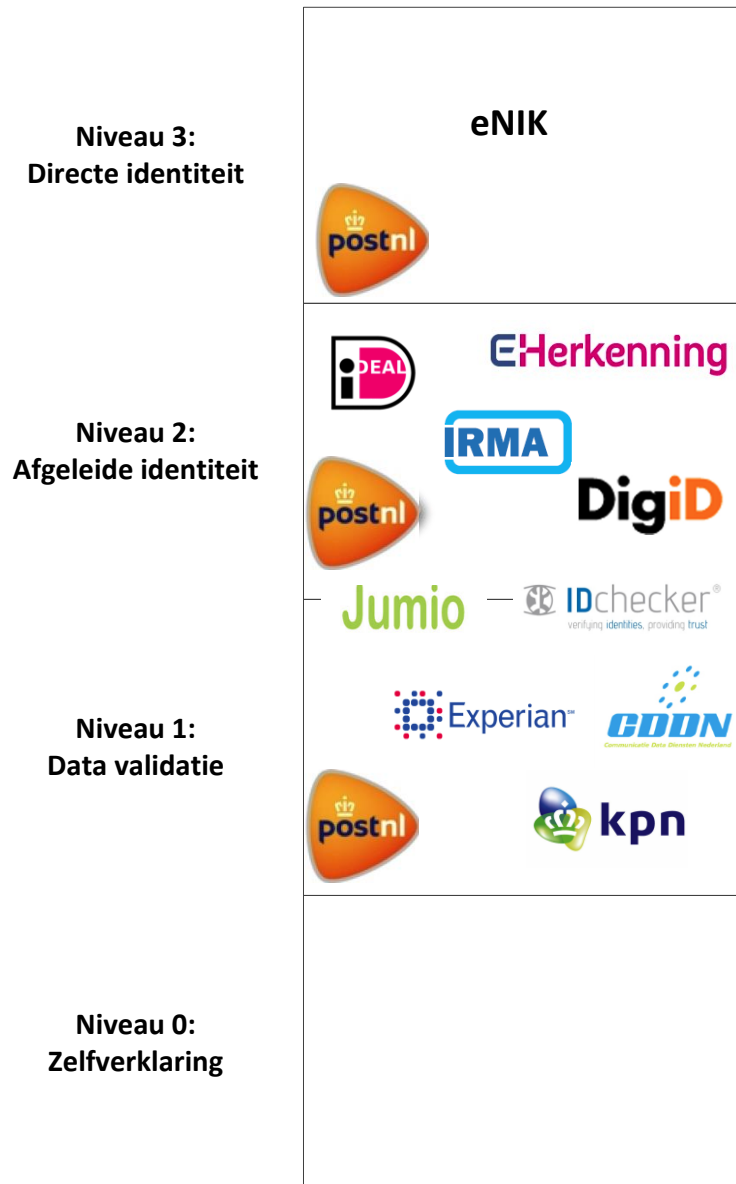
Het hoogste niveau (Niveau 3) betreft een directe controle van een wettelijk identiteitsbewijs. Op dit moment is dat alleen nog maar het geval bij offline controle van het WID document bij aflevering (zoals wordt gedaan door **PostNL**). Online controle op het moment van de transactie wordt pas mogelijk als er een wettelijk online identiteitsdocument beschikbaar komt in de vorm van de **eNIK/eRijbewijs**.

DATAVALIDATIE	AFGELEIDE IDENTIFICATIE	DIRECTE IDENTIFICATIE
Experian	iDEAL	PostNL
KPN	DigiD	eNIK/eRijbewijs
CDDN	eHerkenning	
PostNL	IRMA	
Jumio	PostNL	
IDchecker		

Tabel 12: Datavalidatie, afgeleide en directe identificatieoplossingen

De verschillende oplossingen zijn in figuur 9 grafisch weergegeven per betrouwbaarheidsniveau. Hierin is te zien dat **PostNL** verschillende oplossingen biedt, van datavalidatie via een afgeleide identificatie tot aan de fysieke check van een WID document aan de deur of bij een locatie van **PostNL**.

Een meer gedetailleerde indeling van middelen en diensten voor afgeleide identiteit is de Europese STORK<sup>10</sup> standaard. In dit onderzoek hebben wij niet geprobeerd de verschillende oplossingen te koppelen aan een concreet STORK niveau, onder meer omdat sommige oplossingen nog niet uitontwikkeld zijn en anderen (bijvoorbeeld eHerkenning) meerdere betrouwbaarheidsniveaus ondersteunen. De meer gedetailleerde indeling kan in een vervolgfase alsnog worden gemaakt.



**Figuur 9: Classificering van de oplossingen op betrouwbaarheidsniveau**

<sup>10</sup> Zie <http://www.eid-stork.eu>



## 6.2 Realisatietermijn

De realisatietermijn is de tijd die benodigd is voor realisatie en brede beschikbaarheid van een oplossing. Oplossingen die hier goed op scoren zijn oplossingen die momenteel al beschikbaar zijn voor leeftijdsverificatie. Oplossingen die al voor andere toepassingen beschikbaar zijn, maar nog moet worden aangepast voor leeftijdsverificatie scoren hier minder op. Oplossingen die nog helemaal niet beschikbaar zijn op korte termijn scoren het slechtste.

De oplossingen die momenteel inzetbaar zijn, zijn **CDDN**, **Experian**, **IDchecker** en **PostNL** (check van ID bewijs bij bezorging). Met kleine aanpassingen op korte termijn is de oplossing van **Jumio** te realiseren. Begin 2013 wordt de eerste release van de oplossing van **KPN** verwacht en vanaf april 2013 is **eHerkenning** geschikt voor de uitrol leeftijdsverificatie. Ook **PostNL** geeft aan in Q2 van 2013 een online oplossing op basis van datavalidatie/ afgeleide identificatie gereed te hebben. Oplossingen welke nog langer op zich laten wachten zijn **IDEAL** (vereist aanpassing in systemen van de banken), **DigiD** (vereist besluitvorming gevolgd door aanpassing van systemen), **IRMA** en de **eNIK/eRijbewijs** (vereist aanpassing van wetgeving gevolgd door ontwikkeltraject).

In alle gevallen (met uitzondering van direct beschikbare oplossingen) betreft het hier de meest optimistische schattingen op basis van een positieve businesscase en een snel te realiseren brede uitrol onder de doelgroep.



Figuur 10: Tijdslijn voor realisatietermijn van de oplossingen (indicatief, moment waarop oplossingen op zijn vroegst beschikbaar zijn)

## 6.3 Huidige dekkingsgraad

Het succes criterium huidige dekkingsgraad kijkt voor hoeveel gebruikers de oplossingen momenteel voorhanden zijn. Wordt de oplossing nu al gebruikt voor leeftijdsverificatie of andere toepassingen (bijvoorbeeld betalingen), of als ID in een offline context? Of moeten er nieuwe informatiedragers worden uitgegeven waarop de authenticatiegegevens staan?

De huidige dekkingsgraad is hoog bij twee groepen oplossingen, namelijk de groep die al voor andere doeleinden op internet wordt gebruikt en de groep waarbij de dekkingsgraad hoog is in een offline context. De eerste groep bestaat uit de database oplossingen (**CDDN**,

**Experian** en in de toekomst **KPN** en **PostNL**) en de oplossingen die voor andere doeleinden al online worden gebruikt zoals **iDEAL** voor online betalen en **DigiD** voor online identificatie bij de overheid. De andere groep die hoog scoort op huidige dekkingsgraad bestaat uit oplossingen die gebruik maken van bestaande wettelijke identiteitsbewijzen (**IDchecker**, **Jumio** en de **PostNL** oplossing van WID check aan de deur). De mate waarin de doelgroep voor leeftijdsverificatie (16- tot 18-jarigen) vertegenwoordigd is in bijvoorbeeld bestaande database systemen verschilt wel sterk tussen verschillende oplossingen, daarom scoren sommige oplossingen wat lager (bijvoorbeeld **Experian**, **CDDN**).

Oplossingen waarvoor nog geen authenticatiemiddelen zijn uitgegeven zijn **eNIK/eRijbewijs**, **IRMA** en de e-IDs van **PostNL**, deze scoren daarmee zeer laag op dekkingsgraad. Voor eHerkenning zijn al wel middelen uitgegeven, maar deze zijn niet bedoeld voor leeftijdsverificatie, ook **eHerkenning** scoort op dit criterium dus zeer laag.

## 6.4 Schaalbaarheid

Schaalbaarheid kijkt naar de mate waarin de oplossing inzetbaar is voor andere toepassingen of in andere contexten.

Oplossingen die hier goed op scoren zijn oplossingen waarbij er naast leeftijdsverificatie ook andere diensten mogelijk zijn, of waarbij de oplossingen breed inzetbaar zijn voor meerdere contexten zoals op mobiele telefoons. Alle bekeken oplossingen zijn breder inzetbaar voor e-identity diensten. Bijvoorbeeld **CDDN**, **Experian**, **KPN** en **PostNL** kunnen ook het adres, het telefoonnummer of de kredietwaardigheid van de consument controleren. **iDEAL** is momenteel al geschikt voor online betalen, en **eHerkenning** biedt de mogelijkheid om meerdere attributen te verifiëren welke deels te personaliseren zijn. **eNIK/eRijbewijs** en **IRMA** beogen ook meerdere attributen te kunnen bieden in de toekomst, waarbij **IRMA** de hoogste mate van personalisatie biedt. **IDchecker** en **Jumio** kunnen ook een breder scala aan attributen verifiëren, maar zijn wel beperkt tot de data die op de huidige identiteitsdocumenten staan. **DigiD** wordt nu al gebruikt voor de communicatie tussen de burger en de overheid, maar de schaalbaarheid naar andere attributen zal nog gebouwd moeten worden. Alle oplossingen zijn te gebruiken op de mobiele telefoon, alleen voor de **eNIK/eRijbewijs** is gebruik in combinatie met mobiele apparaten nog in onderzoek.

## 6.5 Begrijpbaarheid / Gemak

Het belangrijkste criterium dat werd genoemd door webwinkeliers is dat een goede oplossing gemakkelijk te begrijpen en te gebruiken moet zijn. Dit wordt bekeken van beide kanten van de tweezijdige markt, dus in hoeverre is de oplossing eenvoudig te implementeren en te gebruiken voor de webwinkel en hoe zit het met het gebruiksgemak voor de klant.

Oplossingen die hier goed op scoren, zijn oplossingen die dicht tegen de offline manier van leeftijdsverificatie aanzitten of die meeliften op handelingen die nu ook al moeten worden verricht bij een internettransactie. De oplossingen die dicht tegen de offline manier van leeftijdsverificatie aanzitten zijn **IDchecker** en **Jumio**, omdat beide oplossingen een ID kaart presenteren aan de webwinkelier via de webcam. Ook voor de webwinkelier lijkt dit op de offline manier van verificatie van de leeftijd. Andere oplossingen welke ook hoog op dit criterium scoren zijn **DigiD** en **iDEAL**, omdat consument deze systemen al gebruikt op het internet. Dit vraagt echter wel een ander soort verificatie vanuit de webwinkelier, omdat hij op het systeem van een 3<sup>e</sup> partij moet aansluiten in plaats van zelf de gegevens te controleren. Dit laatste punt geldt ook voor de trusted databases van **CDDN**, **Experian**, **KPN** en **PostNL**. Bij deze laatste vier partijen vindt de eigenlijke controle achter de schermen plaats op basis van persoonsgegevens die worden ingevuld door de consument, wat een relatief hoge mate van gebruiksgemak geeft. Bij **eHerkenning** komt de gebruikerservaring voor de consument voor een groot deel overeen met die van DigiD of iDEAL, maar ook hier zal de webwinkelier moeten aansluiten op het systeem van een derde partij, de eHerkenningmakelaar.

Controle van ID documenten aan de deur door PostNL is identiek aan andere offline controles, maar omdat dit pas bij de aflevering plaatsvindt is het gebruiksgemak verre van optimaal. Gebruiksgemak van de **eNIK/eRijbewijs** en **IRMA** kaart is nog niet vast te stellen omdat deze oplossingen nog niet bestaan.

## 6.6 Businessmodel

Het criterium businessmodel/betaalbaarheid beschrijft in hoeverre de oplossing gebaseerd is op een realistisch businessmodel. Vele online consumententransacties gaan niet gepaard met hoge bedragen, dus het moet voor de webwinkelier mogelijk zijn om de leeftijd van de consument te checken zonder buitensporige kosten te maken. Met andere woorden: welke oplossingen bieden aanvaardbare implementatiekosten en aanvaardbare kosten per verificatie?

De databasegebaseerde oplossingen (**CDDN**, **Experian**) scoren het beste op dit criterium, omdat zij in staat zijn om bij hogere volumes voor minder dan € 0,02 een verificatie in de database uit te voeren. Ook **iDEAL** scoort goed op dit punt, als we ervan uitgaan dat een iDEAL leeftijdsverificatie vergelijkbaar zal zijn qua prijs met een normale iDEAL transactie (€ 0,10 - € 0,20 bij hogere volumes). Ook **IDchecker** en **Jumio** kunnen tegen relatief lage kosten (in de orde van grootte van € 0,50 – € 2,00 afhankelijk van volumes) een controle op een identiteitsbewijs uitvoeren.

Bij oplossingen waar nieuwe kaarten of andere gegevensdragers moeten worden uitgegeven zullen er implementatie- en opstartkosten moeten worden gemaakt door de consument. Dit

geldt voor middelen van **eHerkenning**, de **eNIK/eRijbewijs**, **IRMA**, en het fysieke e-id van **PostNL**. Voor oplossingen die nog in ontwikkeling zijn (PostNL, eNIK/eRijbewijs, IRMA, KPN) is het vaak nog niet duidelijk hoe het businessmodel eruit ziet. Het is daarom lastig om een harde uitspraak te doen over wat deze oplossingen uiteindelijk gaan kosten.

## 6.7 Privacy / Wetgeving

Dit criterium beschrijft de privacygevoeligheid. In ieder geval moet een oplossing in lijn zijn met geldende wet- en regelgeving rond privacy/bescherming van persoonsgegevens maar sommige oplossingen gaan verder op het gebied van privacy dan andere.

Oplossingen die niet voldoen aan wetgeving zonder dat veranderingen in het systeem worden doorgevoerd zijn **DigiD** en **Jumio**. DigiD is momenteel gebaseerd op het BSN en dat mag niet worden gebruikt door private partijen zoals webwinkels. Ook de oplossing van **Jumio** is nu niet compliant met Nederlandse wetgeving omdat alle scans van WID documenten worden opgeslagen en toegankelijk zijn voor webwinkeliers, wat in strijd is met de wet bescherming persoonsgegevens. Jumio geeft aan dat compliance op korte termijn wel te realiseren is. Voor invoering van de **eNIK/eRijbewijs** zal de wetgeving rond WID documenten moeten worden aangepast om de toevoeging van een chip met persoonsgegevens mogelijk te maken.

Alle oplossingsleveranciers geven aan dat het met hun oplossing mogelijk is om een 'privacy by design' antwoord terug te geven aan de webwinkelier. In geval zal de webwinkelier alleen een ja/nee antwoord terugkrijgen op de vraag of de consument de leeftijd van 16/18 heeft bereikt of niet, in plaats van een exacte geboortedatum of andere gegevens. De oplossingen verschillen in de hoeveelheid data die beschikbaar moet worden gesteld aan de webwinkelier om een verificatie uit te voeren. Optimaal zijn oplossingen waar er zo weinig mogelijk informatie hoeft te worden prijsgegeven aan de webwinkelier. Dit zijn **eHerkenning**, **iDEAL**, **IRMA** en naar verwachting de **eNIK/eRijbewijs**. Ook **DigiD** kan hier hoog scoren mits het wordt aangepast om het BSN niet door te geven aan de webwinkelier.

## 6.8 Veiligheid

Het laatste succescriterium is Veiligheid: in hoeverre is de oplossing beschermd tegen identiteitsfraude en diefstal van persoonsgegevens? Hierbij moet wel een kanttekening worden geplaatst omdat het huidige stadium waar veel van de oplossingen in verkeren het lastig maakt om aan te geven hoe veilig deze precies zullen zijn.

Bij de oplossingen **IDchecker** en **Jumio** is het niet standaard nodig om ook het gezicht van de consument te tonen bij het identiteitsbewijs. Fraude door het tonen van het WID document van iemand anders is daarmee een mogelijkheid. Ook voor de database oplossingen is het

mogelijk om andere gegevens in te vullen (bijvoorbeeld van een van de ouders van een minderjarige) en dan de indruk te wekken bij de webwinkelier dat de leeftijd van 16/18 al bereikt is. Dit vereist wel dat de fraudeur bekend is met alle relevante persoonsgegevens. De oplossingen van **CDDN**, **Experian**, **KPN** en eventueel **PostNL** (zonder fysiek uitgifteproces) zijn vatbaar voor dit type fraude. Oplossingen die de identiteit vaststellen op basis van een real-time authenticatie (**DigiD**, **eHerkenning**, **iDEAL**, **IRMA** en **eNIK/eRijbewijs**) zijn zo veilig als het uitgifteproces dat ervoor wordt gebruikt in combinatie met de Veiligheid van de verbindingen tijdens de authenticatie. Bij uitgifte van een bankkaart (**iDEAL**) wordt altijd een wettelijk ID bewijs gecheckt, bij fysieke uitgifte van een **PostNL** e-ID en een **IRMA** kaart zal dit naar verwachting ook zo zijn. Het uitgifteproces van de **eNIK/eRijbewijs** is nog onduidelijk maar zal naar verwachting vergelijkbaar zijn aan de uitgifte van huidige wettelijke ID-bewijzen. **eHerkenning** maakt gebruik van verschillende betrouwbaarheidsniveaus gebaseerd op STORK. Voor leeftijdsverificatie is ten minste STORK 2 benodigd.

Alle oplossingen maken gebruik van technische maatregelen voor het beschermen van persoonsgegevens tijdens transacties zoals (SSL) encryptie en digitale handtekeningen. Sommige oplossingen zijn gecertificeerd voor hun informatiebeveiliging door externe auditors (**eHerkenning**) of interne auditdiensten (**DigiD**, **iDEAL**).

## 6.9 Overzicht van de gehanteerde modellen

In hoofdstuk 3.2 is een drietal modellen besproken waarmee een systeem/netwerk voor leeftijdsverificatie kan worden georganiseerd. In tabel 14 zijn de verschillende oplossingen voor leeftijdsverificatie geclassificeerd op basis van de modellen.

**IDchecker** en **Jumio** ondersteunen de directe identificatie door de webwinkel door het controleren van een wettelijk ID bewijs als dienst aan te bieden.

Hoe **eNIK/eRijbewijs** en de **IRMA** kunnen worden gebruikt hangt af van de daadwerkelijke implementatie van de oplossing. Daarom zijn deze nog niet opgenomen in de tabel. Sommige van de partijen in de platformcategorie (te weten **CDDN** en **KPN**) hebben aangegeven ook open te staan voor opname in een breder netwerk/Trust Framework.

DIRECT	PLATFORM	TRUST FRAMEWORK
IDchecker	DigiD	eHerkenning
Jumio	Experian	iDEAL
	CDDN	
	PostNL	
	KPN	

Tabel 13: Modellen voor leeftijdsverificatie oplossingen

## 6.10 Samenvatting criteria en oplossingen

Hieronder is grafisch weergegeven hoe de oplossingen zich verhouden tot de criteria betrouwbaarheid en implementatietermijn.



Figuur 11: Betrouwbaarheidsniveau en realisatietermijn

De samenvatting van de scores op alle criteria vindt u hieronder.

	BETROUWBAARHEID	REALISATIETERMIJN	HUIDIGE DEKINGSGRAAD	SCHAALBAARHEID	GEMAK	BUSINESS MODEL	PRIVACY/WET	VEILIGHEID
CDDN	(1) -	++	+	++	+	++	+	+
Experian	(1) -	++	+ -	++	+	++	+	+
KPN	(1) -	+ -	?	++	+	?	+	+
PostNL data	(1) -	+ -	?	++	+	?	+	+
IDchecker	(1) + -	++	++	+	++	+	+	+
Jumio	(1) + -	+	++	+	++	+	+ -	+
eHerkenning	(2) +	+ -	--	+	+	+ -	++	++
iDEAL	(2) +	-	+	++	++	++	++	++
IRMA	(2) +	--	--	++	-	?	++	++
eNIK/eRijbewijs	(3) ++	--	--	?	-	?	+	++
PostNL fysiek	(3) ++	++	++	-	--	+ -	+	+
DigiD	(2) +	-	+	?	++	?	+ -	++

Tabel 14: Samenvatting van criteria en oplossingen

## 7 Conclusie: vier ontwikkelrichtingen voor online leeftijdsverificatie

### 7.1 Conclusie

Aanleiding voor dit onderzoek naar online leeftijdsverificatie op internet was de stroomversnelling waarin de maatschappelijke aandacht voor het onderwerp leeftijdsverificatie de laatste periode is gekomen. Het onderzoek geeft antwoord op de vraag of er haalbare oplossingen zijn om op korte termijn online leeftijdsverificatie in Nederland op een brede schaal toe te passen, anders dan te wachten op de eNIK of een aanpassing van iDEAL. Twaalf potentiële oplossingen (*Experian, iDEAL, KPN, DigiD, CDDN, eHerkenning, PostNL, IRMA, Jumio, eNIK/eRijbewijs, IDchecker* en *Banken*) zijn daarvoor geanalyseerd en getoetst op eerder beschreven randvoorwaarden en succescriteria.

Er zijn vele overeenkomsten tussen leeftijdsverificatieoplossingen. De besproken criteria geven aan waar de verschillen liggen, maar er zijn ook verschillende overeenkomsten welke belangrijk zijn voor de haalbaarheid, maar niet onderscheidend zijn. Alle bekeken systemen zijn bijvoorbeeld geschikt voor een breder scala aan identiteitsdiensten dan alleen leeftijdsverificatie, bijvoorbeeld adresvalidatie. Een dergelijke brede propositie is een belangrijke succesfactor voor de langere termijn. Verder is het ook belangrijk dat er voldoende toegevoegde waarde wordt geleverd voor een acceptabele prijs. Ook dit business case-aspect wordt goed ingevuld door de meeste oplossingen: de (verwachte) vraagprijs staat in verhouding tot de aangeboden diensten. Daarnaast is het belangrijk dat de consument zijn eigen gegevens kan beheeren en dataminimalisatie de norm is. Deze vorm van privacy-by-design is belangrijk voor de privacy van de consument en de meeste oplossingen voldoen hier aan, of geven aan naar deze richting te bewegen. Datavalidatie diensten (niveau 1) zijn soms een uitzondering, maar deze diensten voldoen in ieder geval aan de eisen van de wet bescherming persoonsgegevens. Tot slot voldoen alle oplossingen aan de verwachte eisen voor informatiebeveiliging (al is dat bij de oplossingen die nog niet in de praktijk werken lastig na te gaan).

Concluderend kan gesteld worden dat er een ruim aanbod is van potentiële oplossingen voor online controle van de leeftijd van de consument. De keuze voor een oplossing of groep oplossingen is sterk afhankelijk van de eisen die belanghebbenden stellen aan de betrouwbaarheid van leeftijdsverificatie en de gewenste termijn waarop een oplossing beschikbaar moet zijn.

Er zijn globaal vier ontwikkelrichtingen, die afhankelijk zijn van de keuze voor één van de in paragraaf 3.1 besproken betrouwbaarheidsniveaus. Combinaties van deze verschillende scenario's zijn daarbij ook mogelijk:



- A. Handhaven status quo** De eerste optie is om genoeg te nemen met zelfverklaringen. Dit betekent niets veranderen aan de huidige situatie en doorgaan met de manier waarop leeftijdsverificatie vandaag de dag gebeurt op het internet. Hierbij is een eigenverklaring door de consument de norm, mogelijk aangevuld met controle bij levering in het geval van aankoop van fysieke goederen.
- B. Quick win, best effort** Indien er wordt gekozen voor datavalidatie als acceptabel betrouwbaarheidsniveau, kan op zeer korte termijn van start worden gegaan. Deze oplossingen zijn niet door de overheid uitgegeven, maar hebben wel een korte realisatietermijn en potentieel groot bereik. Oplossingen die momenteel hiervoor geschikt zijn, zijn IDchecker, Experian, CDDN, en in de nabije toekomst KPN, PostNL en Jumio. Dit levert een grote verbetering van de betrouwbaarheid ten opzicht van de huidige situatie (optie A), waarin vaak helemaal geen leeftijdsverificatie plaats kan vinden. Op termijn zouden deze oplossingen vervangen of aangevuld kunnen worden door real-time authenticatieoplossingen (optie C) en/of de eNIK danwel het eRijbewijs (optie D).
- C. Aanpassing van bestaande authenticatieproducten** De derde optie is om te kiezen voor oplossingen die gebaseerd zijn op een afgeleide authenticatie gebaseerd op een WID-document ergens in het proces. Het gaat dan om oplossingen welke nu al bereik hebben (hoewel niet al deze systemen een even groot bereik hebben onder de doelgroep van 16-18 jarigen) en een bestaand uitgifteproces en vertrouwde gebruikerservaring, zoals iDEAL en DigiD. Deze oplossingen moeten nog wel geschikt gemaakt worden voor online leeftijdsverificatie. Het aanpassen van de systemen en/of registreren van voldoende gebruikers zal in alle gevallen zeker 1-2 jaar duren. Invoeren van geheel nieuwe middelen, zoals de IRMA kaart of eHerkenning middelen voor leeftijdsverificatie, zal naar verwachting langer duren. Invoering zal in alle gevallen meer investeringen eisen dan de oplossingen uit optie 1. Daar staat tegenover dat de afgeleide identificatieoplossingen een hogere mate van betrouwbaarheid kunnen bieden (afhankelijk van het gebruikte uitgifteproces) en een groter bereik (mits wordt gekozen voor een middel dat laagdrempelig beschikbaar is voor alle consumenten in de doelgroep).
- D. Wettelijk verplicht middel op lange termijn** Tot slot de laatste mogelijkheid is om te wachten op het hoogste betrouwbaarheidsniveau en een wettelijk identificatiemiddel. De beoogde overheidsoplossing is een hoog niveau middel in het eID stelsel (eNIK/eRijbewijs), vandaar ook dat dit de oplossing is die door het ministerie als kansrijk wordt genoemd (zie Inleiding). Het grote nadeel van deze oplossingsrichting is dat de eNIK nog zeker 2-3 jaar op zich laat wachten en mogelijk langer, afhankelijk van de invoeringsstrategie die wordt gekozen. In de tussentijd blijft leeftijdsverificatie in hetzelfde grijze gebied waar het nu is tenzij ook voor andere oplossingsrichtingen wordt gekozen naast eNIK/eRijbewijs.

Concluderend kan gesteld worden dat er een duidelijke keuze gemaakt moet worden voor een acceptabel betrouwbaarheidsniveau enerzijds en een acceptabele termijn voor realisatie anderzijds. Op alle bekeken betrouwbaarheidsniveaus zijn één of meer systemen beschikbaar die voldoen aan minimale wettelijke- en veiligheidseisen en die een stap vooruit zijn ten opzichte van de huidige situatie (optie A). Dit is grafisch weergegeven in figuur 11 in het vorige hoofdstuk. Wanneer de gewenste haalbaarheidstermijn en benodigde betrouwbaarheidsniveau duidelijk zijn gaan criteria van de verschillende stakeholders een rol spelen in de daadwerkelijke keuze voor de beste oplossing.

De branchevereniging van webwinkeliers Thuiswinkel.org heeft aangegeven dat het bereik en de conversie tegen acceptabele kosten de belangrijkste criteria zijn voor webwinkeliers. Hierbij geldt bovendien dat oplossingen die gecombineerd kunnen worden in een trust framework het meest kansrijk zijn omdat dit ervoor zorgt dat webwinkelier eenvoudig aan kunnen sluiten zonder heel veel verschillende oplossingen zelf te hoeven ondersteunen, terwijl consumenten hun bestaande middelen kunnen hergebruiken bij verschillende webwinkels. Het is al met al zeker niet zo dat wachten op invoering van de eNIK de enige haalbare optie is voor online leeftijdsverificatie.

## **7.2 Toekomstbeeld voor online identificatie**

Online leeftijdsverificatie van een consument is een specifieke invulling van het algemene probleem van online identificatie en authenticatie van (kenmerken van) de consument.

Er is een analogie te maken met de markt voor online betaalmethodes van een decennium terug. Deze markt was toen, net als de markt voor identificatiediensten nu, in de opstartfase. Veel verschillende betaalmethodes werden naast elkaar gelanceerd met ieder hun eigen voor en nadelen op het gebied van bereik, kosten en gebruiksgemak. Vanuit de wildgroei aan betaalmethodes op internet ontstonden payment service providers (PSPs) die het mogelijk maken voor webwinkels om op eenvoudige wijze de consument meerdere methodes aan te bieden. Uiteindelijk werd de meest succesvolle betaalmethode in Nederland iDEAL, ontstaan vanuit het hergebruik van de bestaande authenticatiemethodes voor online bankieren en gebaseerd op de samenwerking van alle consumentenbanken in een vierpartijenmodel (Trust Framework).

Dit zou ook het toekomstbeeld kunnen zijn voor online verificatiediensten: Identity service providers of identity brokers kunnen de complexiteit voor een webwinkel weghalen door eenvoudige toegang te bieden tot meerdere identiteitsdiensten. Binnen het stelsel voor eHerkenning wordt een dergelijke serviceprovider een 'herkenningsmakelaar' genoemd. Op

termijn kan door marktwerking een identificatiemethode het meeste marktaandeel verwerven, mogelijk een aangepaste versie van een al bestaand systeem, of verschillende methodes die samen een netwerk (Trust Framework) vormen.

Daarbij zijn er twee cruciale verschillen tussen de markt voor betaalsystemen en voor leeftijdsverificatie die in acht moeten worden genomen. Ten eerste is betalen een noodzaak voor de consument en de winkelier om de transactie te voltooien, terwijl leeftijdscontrole een extern (door de wetgever) opgelegde plicht is. Zolang gedoogd wordt dat webwinkeliers genoegen nemen met een zelfverklaring over de leeftijd is er voor winkeliers en consumenten geen animo om meer betrouwbare methodes te gaan gebruiken. Het tweede verschil is dat op het gebied van online identificatie de overheid zelf ook een leverancier van oplossingen is. Op dit moment is DigiD weliswaar niet een beoogde oplossing binnen het private domein, maar de eNIK/ het eRijbewijs worden wel zo gepositioneerd en kunnen op die manier een rem houden op ontwikkeling/acceptatie van alternatieve oplossingen door het bedrijfsleven.

Om leeftijdsverificatie in Nederland breed in te voeren zijn de technische oplossingen per direct of op afzienbare termijn beschikbaar, zoals blijkt uit de analyse van een representatieve doorsnede van (potentiële) oplossingsaanbieders. De belangrijkste randvoorwaarden voor verdere doorvoering zijn daarmee:

1. Duidelijkheid vanuit de wetgever over de eisen aan webwinkeliers. Wordt de huidige gedoogconstructie gehandhaafd tot de eNIK beschikbaar is, of zijn andere betrouwbaarheidsniveaus acceptabel met een kortere realisatietermijn?
2. Gebruiksgemak en bereik zijn cruciaal voor succesvolle oplossingen. Webwinkeliers zullen geen gebruik maken van methodes die niet beschikbaar zijn voor de doelgroep (te weinig bereik) of die zo ingewikkeld zijn dat de consument afziet van de transactie (te weinig gebruiksgemak). Er ligt hier een rol voor identity service providers / brokers om webwinkeliers te helpen.
3. Positieve businesscase. Leeftijdsverificatie is een wettelijk opgelegde verplichting en daarmee een kostenfactor voor de webwinkel. De kosten van een verificatie moeten per transactie daarom laag genoeg blijven ten opzichte van het transactiebedrag of de businesscase moet gemaakt worden op basis van aanvullende identiteitsdiensten.
4. Uitbreidbaarheid naar andere identificatiediensten. Het bouwen of aanpassen van een systeem alleen om daar leeftijdsverificatiediensten mee te kunnen doen zal niet snel leiden tot een positieve businesscase. Als hetzelfde systeem ook geschikt is voor andere identificatievragen (bijv. geverifieerd adres) dan wordt de drempel voor invoering al een stuk lager. Positief is dat alle door ons onderzochte verificatiediensten ook bredere dienstverlening ondersteunen.

### 7.3 Aanbevelingen en vervolgstappen

Deze marktverkenning toont aan dat er meer dan genoeg aanbieders zijn van diensten en systemen die (potentieel) voor leeftijdsverificatie geschikt zijn en een verbetering kunnen bieden in de online context ten opzichte van de status quo. Om dichter bij het eerder geschetste toekomstbeeld te komen worden de volgende stappen aanbevolen:

1. Een eerste aanbeveling is om verschillende opties verder uit te werken waarlangs leeftijdsverificatie zich kan ontwikkelen. Na deze eerste marktverkenning van de aanbodkant van e-identity is het nuttig om dieper in te gaan op de vraagkant: welke van de bekeken factoren zijn echt kritieke succesfactoren voor consumenten en webwinkels? Welke combinaties van oplossingen zijn mogelijk? Dit zou verder getoetst moeten worden bij alle betrokken stakeholders.
2. Een tweede aanbeveling is om de marktverkenning uit te breiden naar overige oplossingen. Hoewel dit rapport een representatief beeld geeft, verdient het aanbeveling om ook andere Nederlandse oplossingen nader te bekijken zoals van Qiy ([www.qiy.nl](http://www.qiy.nl)) en Prooflink ([www.prooflink.com](http://www.prooflink.com)). Daarnaast moeten oplossingen worden bekeken die in de ons omringende landen en in de rest Europa gebruikt worden en wellicht in Nederland herbruikbaar zijn. Let hierbij wel op dat veel oplossingen slecht te importeren zijn vanwege verschillen in wetgeving rond bijvoorbeeld privacy.
3. De derde aanbeveling richt zich op de overheid. De overheid moet eisen formuleren aan private initiatieven en duidelijkheid scheppen over beoogde handhaving. Uit de communicatie met webwinklers is gebleken dat afwezigheid van handhaving een van de belangrijkste redenen is om slechts beperkt aandacht te geven aan leeftijdsverificatie ten opzichte van andere e-identiteitsdiensten. De overheid als wetgever moet duidelijke richtlijnen stellen waar private initiatieven aan moeten voldoen, en ook moet zij helderheid verschaffen over het beoogde handhavingsbeleid.
4. Tot slot is het belangrijk om de maatschappelijke discussie te voeren over leeftijdsverificatie op internet. Tot nu toe wordt die geblokkeerd doordat partijen wachten op overheidsoplossingen (eNIK/eRijbewijs) en in de tussentijd genoeg nemen met zelfverklaringen of andere beperkt toepasbare maatregelen. In afwachting van een definitieve oplossing op lange termijn zou met belanghebbenden moeten worden gekeken hoe gewerkt kan worden met de nu beschikbare middelen. Pilots/Proof of Concept projecten kunnen hier input voor leveren. Als platform voor bedrijfsleven, overheid en internetsamenleving kan ECP hier een belangrijke aanjagende rol vervullen.

## Bijlage 1: Overzicht leeftijdsgebonden producten

PRODUCT/ DIENST	LEEFTIJD	EXTRA INFORMATIE	HUIDIGE SITUATIE	VOORBEELD BEDRIJF
Alcoholische drank	16/18+	Afleveradres	Controle bij aflevering	Albert.nl
Adult producten	18+	Afleveradres	Leeftijd 18 + wordt gevraagd (zelfverklaring)	Pabo.nl
DVD	6/9/12/16+	Afleveradres	Geen leeftijdscheck	Bol.com
TV herhalingen	6/9/12/16+		16+ alleen beschikbaar na 22:0011	Publieke omroep, RTL
Games	3/7/12/16/18+	Afleveradres	Geen leeftijdscheck	Bol.com
Online gokken/wedden	18+	Account gegevens	Leeftijd op site moet > 18 zijn	Oranje casino, Kroon
Bankrekening aanvragen	Bank afhankelijk	Persoonsgegevens, BSN, rijbewijs/paspoort	RABO: online aanvragen, papieren overeenkomst ondertekenen ABN: afspraak online, komt iemand langs	ING, Rabobank, SNS
Mobiel abonnement	18+	Account informatie, persoonsgegevens, document nummer identiteitsbewijs	Leeftijd op site moet > 18 zijn	Belcompany, Vodafone, KPN
Identiteitsdocumentatie & rijbewijs	Exacte leeftijd	Eventueel goedkeuring CBR, BSN nummer, persoonsgegevens	Niet mogelijk	Gemeenten
Fora	Leeftijdsafhankelijke fora B.v. <12,16,18	Inloggegevens, geslacht	Invullen van de leeftijd/geslacht	Fok.nl, viva.nl, tienerforum

Tabel 15: Overzicht van leeftijdsgebonden producten

<sup>11</sup> Geldt alleen voor [www.uitzendinggemist.nl](http://www.uitzendinggemist.nl)